

# Free Left Distributive Algebras and a Canonical Extension

Scott Cramer      Meng-Che “Turbo” Ho\*  
Sheila K. Miller Edwards      Nam Trang<sup>†‡</sup>

## Abstract

Assuming a large cardinal hypothesis, Laver gave a representation of the monogenerated free left distributive algebra (LDA) using elementary embeddings and used this representation to prove many algebraic results. Some of these results were later proved by Dehornoy in ZFC, without the large cardinal hypotheses. However, there is an important algebraic result whose consistency strength is unknown [17, 8]. Recent results [1] extend the connection between elementary embeddings of set theory and free LDAs to the many-generated case.

Assuming large cardinals, we prove two results. First, we prove that finitely-generated free LDAs with distinct numbers of generators are  $\Sigma_1$ -elementarily equivalent but not  $\Sigma_2$ -elementarily equivalent. We also prove a partial structural analogue to Laver’s representation of LDAs. We construct an extension of the monogenerated free LDA where application by any fixed element is an elementary embedding of LDAs. We argue that this extension is canonical by demonstrating homogeneity and universality properties. These results also provide additional examples of algebraic properties provable from large cardinals without known proofs from the standard axioms of set theory.

## 1 Introduction

Left distributive algebras are those in which multiplication on the left by an element of the algebra is a homomorphism: In a left distributive algebra with underlying set  $A$  and binary operation  $\cdot$ , for every element  $a, b$ , and  $c$ , the equality  $a \cdot (b \cdot c) = (a \cdot b) \cdot (a \cdot c)$  holds. Many well-known mathematical operations, including group conjugation and the weighted mean, are left distributive. In

---

\*The second author acknowledges support by the National Science Foundation under Award No. 2054558 and No. 2555186.

†The fourth author acknowledges support by the National Science Foundation under Career Award No. 1945592.

‡The project began at a SQuaRE at the American Institute of Mathematics. The authors thank AIM for providing a supportive and mathematically rich environment.

each of these cases, the operation is also idempotent ( $x \cdot x = x$  for every element  $x$  in the algebra), hence the algebras are not free.

Beginning in the 1980s, a deep connection was discovered between left distributive algebras and large cardinals, logical axioms the existence of which implies the consistency of the usual axioms of set theory, ZFC (and also many statements independent of ZFC). By Gödel's Incompleteness Theorems, the consistency of large cardinal axioms does not follow from ZFC. Large cardinal axioms are linearly ordered by consistency strength,<sup>1</sup> and the stronger large cardinal axioms can typically be formulated to assert the existence of elementary embeddings with specific closure properties. Under one such large cardinal hypothesis called a *rank-to-rank* embedding, Richard Laver [15] proved that the algebra generated by the closure of a single rank-to-rank embedding under the *application* operation is linearly ordered by the iterated left subterm relation  $<_L$  and isomorphic to the free left distributive algebra on one generator,  $\mathcal{A}$ . (For details, see Section 2.) In so doing, Laver proved that the word problem for the left distributive law is decidable.

Patrick Dehornoy subsequently proved that the decidability of the word problem is a purely algebraic result not requiring large cardinals [6]. In particular, he defined an operation on elements of Artin's braid group on infinitely many strands  $B_\infty$  and showed in ZFC that the closure of any element of  $B_\infty$  under that operation is isomorphic to the free left distributive algebra on one generator,  $\mathcal{A}$ . (See Section 2.)

Work to generalize and extend these early results and to better understand the relationship between large cardinals and left distributive algebras has continued since the 1990s. Also using Artin's braid group, David Larue significantly simplified Dehornoy's proof [13] and constructed free left distributive algebras on  $n$  generators for each finite  $n$ , now called the Larue groups [14]. Though it seemed that an example of a many-generated free left distributive algebra should also exist in the context of rank-to-rank embeddings, the demonstration of such an algebra proved elusive until quite recently [1, 2]. Many questions from the 1990s remain open, including one about the consistency strength of a theorem about a family of finite algebras known as the Laver tables.

Perhaps the central question of the theory of left distributive algebras is whether there are statements in the theory of left distributive algebras that contain large cardinal strength—namely, statements the assertion of which implies the existence of a large cardinal—or whether all structural properties of left distributive algebras can be proven from the usual axioms of set theory (or from considerably weaker theories). Our overarching goal is to understand which of these two possibilities holds. This paper contributes two further structural results on left distributive algebras derivable from large cardinals. First, we show that finitely-generated free left distributive algebras on distinct numbers of generators are  $\Sigma_1$ -elementarily equivalent but not  $\Sigma_2$ -elementarily equivalent; second, we define a left distributive algebra  $\mathcal{C}_1$  that preserves more properties of algebras of rank-to-rank embeddings than does the monogenerated free left

---

<sup>1</sup>All natural large cardinal axioms of interest to set theorists are linearly ordered.

distributive algebra  $\mathcal{A}$ . Whether it is possible to prove either of the two main results of this paper without large cardinal hypotheses is open.

The first of our two main results shows, under a large cardinal hypothesis, that, in spite of the qualitative differences between working with one- and many-generated free left distributive algebras,  $\Sigma_1$  formulas cannot distinguish between finitely-generated, free left distributive algebras with different numbers of generators, while  $\Sigma_2$  formulas can.

**Theorem (A).** *Under appropriate large cardinal assumptions, for any two distinct positive integers  $m$  and  $n$ , the free left distributive algebras on  $m$  and  $n$  generators,  $\mathcal{A}_m$  and  $\mathcal{A}_n$ , are  $\Sigma_1$ -elementarily equivalent but not  $\Sigma_2$ -elementarily equivalent.*

Laver's result that the algebra  $\mathcal{A}_{\{j\}}$  generated by closing a single rank-to-rank elementary embedding  $j$  under the application operation is free can be viewed as asserting that  $\mathcal{A}_{\{j\}}$  always embeds into a simply defined algebraic structure (namely, the free left distributive algebra on a single generator). His result suggests a natural question: Does the closure of every finite set of rank-to-rank embeddings generate an algebra that embeds into a simply definable structure (such as the free left distributive algebra on the appropriate number of generators)?

The algebras generated by finite collections of rank-to-rank embeddings are more complex than  $\mathcal{A}_{\{j\}}$  and so, too, is the answer to this question. Much of the time, it is not clear what the algebra generated by two embeddings might look like. However, under special circumstances, it is possible to find two embeddings that do generate an algebra isomorphic to the free, two-generated left distributive algebra  $\mathcal{A}_2$  [1]. Indeed, for any cardinal  $\kappa$ ,  $1 \leq \kappa \leq 2^{\aleph_0}$ , we can find a collection of elementary embeddings that generate the free left distributive algebra  $\mathcal{A}_\kappa$  [2].

Motivated to capture additional structure of the large cardinal embeddings, we extend the free left distributive algebra  $\mathcal{A}$  to a canonical algebra  $\mathcal{C}_1$  and show that  $\mathcal{C}_1$  has certain desirable properties. The demonstration of these properties is the second of our two main results.

**Theorem (B).** *Under appropriate large cardinal assumptions, the structure  $\mathcal{C}_1$  is universal and homogeneous, and the application operation on  $\mathcal{C}_1$  is elementary. Furthermore, certain sets of elementary embeddings that do not embed into  $\mathcal{A}$  do embed into  $\mathcal{C}_1$ .*

See Corollary 62 for the precise meaning of universal in the statement Theorem B, Corollary 61 for that of homogeneous, and Theorem 63 for details of which sets of elementary embeddings embed into  $\mathcal{C}_1$ . The large cardinal assumptions used in Theorems (A) and (B) are precisely stated later in the paper.

Our theorem shows that the map from  $\mathcal{A}$  to  $\mathcal{A}$  given by application by an element  $a$  in  $\mathcal{A}$  can be extended to an elementary embedding from the expanded algebra  $\mathcal{C}_1$  to  $\mathcal{C}_1$ . Laver started with a (set-theoretic) elementary embedding and obtained an LDA; we begin with the application operation on LDAs, which are

purely algebraic objects, and obtain, using large cardinals, the existence of a purely algebraic elementary embedding of LDAs.

The structure of the remainder of the paper is as follows. Section 2 gives relevant background in model theory and large cardinal theory and a brief summary of important results about left distributive algebras. In Section 3 we prove a theorem connecting divisibility conditions in the algebra  $\mathcal{A}$  to the existence of pullbacks in the algebra  $\mathcal{A}_{\{j\}}$  of embeddings. In Section 4 we show that the finitely-generated free left distributive algebras are all  $\Sigma_1$ -elementarily equivalent to one another but not  $\Sigma_2$ -elementarily equivalent (Theorem (A)). We then define a canonical extension  $\mathcal{C}_1$  of  $\mathcal{A}$  in Section 5 and prove that  $\mathcal{C}_1$  preserves additional (relative to  $\mathcal{A}$ ) properties of the large cardinal embeddings (Theorem (B)). We close with open questions and possible extensions of this work in Section 6.

## 2 Background

Here we offer a brief overview of relevant results about left distributive algebras (LDAs) and their connections to large cardinal axioms. For a comprehensive treatment of the subject, especially self-distributivity and braids, see [7]. For a concise survey, see [19].

### 2.1 Large Cardinals

As mentioned in the introduction, large cardinals are strong logical axioms in the form of cardinals that, if they exist, imply the consistency of ZFC. The large cardinal axioms are (as far as anyone has been able to prove) linearly ordered by consistency strength, and the largest of the large cardinals can be formulated to assert the existence of nontrivial elementary embeddings  $j$  from the universe of sets  $V$  to a transitive model of set theory  $M$  that agrees with  $V$  on a large collection of sets. Such elementary embeddings preserve much of the structure of the domain,  $V$ , and the closer the target model  $M$  is to  $V$  (or, more generally, the domain), the stronger the large cardinal assertion. Let us now be precise about the definition of an elementary embedding.

Recall that a language  $\mathcal{L}$  may include symbols for constants, functions, and relations; an  $\mathcal{L}$ -structure is a set in which interpretations of the constants, functions, and relations have been assigned. An elementary embedding between  $\mathcal{L}$ -structures preserves *all* first-order formulas in the language. The language of set theory  $\{\in\}$  contains a single binary relation symbol  $\in$  interpreted as set membership. An elementary embedding  $j$  from  $\langle V, \in \rangle$  to a transitive substructure  $\langle M, \in \rangle$  preserves every first-order formula  $\varphi(v_1, \dots, v_n)$  in the language  $\{\in\}$  of set theory.

**Definition 1.** Say  $j$  is an elementary embedding from  $\langle V, \in \rangle$  to a transitive substructure  $\langle M, \in \rangle$  if and only if, for every first-order formula  $\varphi(v_1, \dots, v_n)$

and every tuple  $a_1, \dots, a_n$  of elements of  $V$ ,

$$V \models \varphi[a_1, \dots, a_n] \Leftrightarrow M \models \varphi[j(a_1), \dots, j(a_n)].$$

A nontrivial elementary embedding is one that is not the identity and thus must move some ordinal  $\alpha$ . We will consider only nontrivial elementary embeddings. For a nontrivial elementary embedding  $j$ , call the least cardinal  $\kappa$  moved by  $j$  the *critical point* of  $j$ , denoted by  $\text{crit}(j)$ . Letting  $\kappa = \text{crit}(j)$ , observe that, by elementarity,  $\kappa$  must be less than its image:  $\kappa < j(\kappa)$ . Repeatedly applying  $j$  to the image of  $\kappa$  under  $j$  we get the *critical sequence of  $j$* ,  $\overrightarrow{\text{crit}}(j)$ :

$$\kappa = \kappa_0, j(\kappa_0) = \kappa_1, \dots, j(\kappa_n) = \kappa_{n+1}, \dots$$

Recalling the right power notation from the previous section, note that  $\kappa_n = \text{crit } j^{(n)}$ . To make reference to the collection of all critical points of embeddings in  $\mathcal{A}_j$ , we define

$$\text{crit } \mathcal{A}_j = \{\kappa : \exists k \in \mathcal{A}_j (\text{crit}(k) = \kappa)\}.$$

It is natural to wonder how similar the target model  $M$  can be to the whole universe of sets  $V$ . Maximal similarity would be for  $M$  to be  $V$  itself: Say  $\kappa$  is a *Reinhardt cardinal* if it is the critical point of a nontrivial elementary embedding  $j : V \rightarrow V$ .<sup>2</sup> As we will see now, Reinhardt cardinals are not consistent with the Axiom of Choice.<sup>3</sup>

**Theorem 2** (Kunen). *Assuming ZFC is consistent, there are no Reinhardt cardinals. Indeed, assuming the Axiom of Choice, for no ordinal  $\lambda$  does there exist a nontrivial elementary embedding  $j : V_{\lambda+2} \rightarrow V_{\lambda+2}$ .*

See [12] for several proofs of Kunen’s Theorem. The first statement of Theorem 2 is the original form of Kunen’s Theorem; the second is a corollary. A remarkable recent result of Schlutzenberg, [22], shows that the theory  $ZF +$  “there is a non-trivial embedding  $j : V_{\lambda+2} \rightarrow V_{\lambda+2}$ ” is consistent relative to a very strong large cardinal hypothesis called  $I_0$ .

While there are limits to the closure of the target model if we assume ZFC, some amount of closure of an elementary embedding is guaranteed: For every nontrivial elementary embedding  $j : V \rightarrow M$  with  $M$  transitive and  $\text{crit}(j) = \kappa$ ,  $M$  necessarily contains  $V_{\kappa+1}$  as a subset. (See, for example, [1] for a proof of this fact.)

A cardinal  $\kappa$  that is the critical point of a nontrivial elementary embedding  $j : V \rightarrow M$  is called a *measurable cardinal*. If the image  $M$  contains all of its own  $\lambda$ -sequences for some  $\lambda > \kappa$ , it is called  *$\lambda$ -supercompact*. If it is closed under subsets of size  $j(\kappa)$ , it is called *huge*. In the stated order, these axioms

<sup>2</sup>The definition of a Reinhardt cardinal takes place in von Neumann–Gödel–Bernays class theory, which allows quantification over classes, rather than in ZFC.

<sup>3</sup>It is not known whether Reinhardt cardinals under  $ZF + \neg AC$  are inconsistent, and there are many axioms that trade the Axiom of Choice for closure beyond the limit of compatibility with AC given by Kunen’s Theorem. For more on this see, for example, [10, 9].

are progressively stronger in consistency strength, and there are many others between and beyond them. The axioms of interest to us here are those for which the domain and target models are both rank initial segments of the universe  $V_\delta$  for some ordinal  $\delta$ . Such cardinals are larger than huge cardinals.

For  $\lambda$  a limit ordinal of cofinality  $\omega$ , a nontrivial elementary embedding  $j : V_\lambda \rightarrow V_\lambda$  is a *rank-to-rank* embedding, also called an  $I_3$  embedding. We frequently talk about the collection of all such embeddings, so we reiterate the following definition.

**Definition 3.** Suppose  $\lambda$  is a limit ordinal of cofinality  $\omega$ . Define  $\mathcal{E}_\lambda$  to be the set of nontrivial elementary embeddings  $j : V_\lambda \rightarrow V_\lambda$ .

There are a number of ways to incrementally strengthen the rank-to-rank hypothesis without exceeding the known threshold at  $\lambda + 2$  for inconsistency with the Axiom of Choice. In essence, each level of the strengthening preserves progressively more complex formulas. We give the definitions of these levels below and will use some of them extensively in the sequel, but before stating them, we offer a brief review of the Levy hierarchy of formulas for first-order languages  $\mathcal{L}$  and the language of set theory  $\mathcal{L}_\in$ .

For a first-order language  $\mathcal{L}$ , a quantifier-free formula is considered both  $\Sigma_0$  and  $\Pi_0$ . If the formula  $\psi$  is  $\Sigma_n$ , then the formula  $\forall v_1 \dots \forall v_k \psi$  is  $\Pi_{n+1}$ , and, likewise, if  $\psi$  is  $\Pi_n$ , then  $\exists v_1 \dots \exists v_k \psi$  is  $\Sigma_{n+1}$ .

For  $\mathcal{L}_\in$ , an existential formula  $\varphi$  in which all quantifiers are bounded ( $\exists v \in w$ ) is called  $\Sigma_0$ . Similarly, a universal formula  $\varphi$  with only bounded quantifiers ( $\forall v \in w$ ) is  $\Pi_0$ . If the formula  $\psi$  is  $\Sigma_n$ , then the formula  $\forall v_1 \dots \forall v_k \psi$  is  $\Pi_{n+1}$ , and, likewise, if  $\psi$  is  $\Pi_n$ , then  $\exists v_1 \dots \exists v_k \psi$  is  $\Sigma_{n+1}$ .

**Definition 4.** Say that an elementary embedding  $j$  from  $\mathcal{M}$  to  $\mathcal{N}$  is  $\Sigma_m$ -elementary if for all  $\Sigma_m$ -formulas  $\varphi(v_1, \dots, v_k)$  and all  $x_1, \dots, x_k$  in  $\mathcal{M}$ ,

$$\mathcal{M} \models \varphi[x_1, \dots, x_k] \text{ if and only if } \mathcal{N} \models \varphi[j(x_1), \dots, j(x_k)].$$

Two  $\mathcal{L}$ -structures  $A$  and  $B$  are *n-equivalent*, denoted by  $A \equiv_n B$  and also called  *$\Sigma_n$ -equivalent*, if every  $\Sigma_n$ -sentence (equivalently, every  $\Pi_n$ -sentence) is true in  $A$  if and only if it is true in  $B$ . Say  $A$  and  $B$  are *elementarily equivalent*, denoted by  $A \equiv B$ , if every (first-order) sentence is true in  $A$  if and only if it is true in  $B$ .

In the case that  $\mathcal{M}$  and  $\mathcal{N}$  are sets, we similarly define  $\Sigma_n^1$ -elementary, using second-order quantifiers (that is, quantifying over subsets).

It is now possible to define the strengthenings of I3 mentioned earlier. The embeddings here are given in order of increasing consistency strength.

**Axiom I3:** There exists a nontrivial elementary embedding  $j : V_\lambda \rightarrow V_\lambda$ .

**Axiom I2:** There exists a nontrivial elementary embedding  $j : V \rightarrow M$  for some transitive class  $M$  such that the supremum of the critical sequence of  $j$  is  $\lambda$  and  $V_\lambda \subseteq M$ .

$\Sigma_n^1$ -**elementary rank-to-rank** There exists a nontrivial  $\Sigma_n^1$ -elementary embedding  $j : V_\lambda \rightarrow V_\lambda$ .<sup>4</sup>

**Axiom I1:** There exists a nontrivial (fully) elementary embedding  $j : V_{\lambda+1} \rightarrow V_{\lambda+1}$ .

**Axiom I0:** There exists a nontrivial elementary embedding

$$j : L(V_{\lambda+1}) \rightarrow L(V_{\lambda+1}).<sup>5</sup>$$

We now turn to the application operation.

**Definition 5** (Application). Let  $j : V_\lambda \rightarrow V_\lambda$  be a rank-to-rank embedding. For  $A \subseteq V_\lambda$ , define

$$j \cdot A = jA = j(A) = \bigcup_{\alpha < \lambda} j(A \cap V_\alpha).$$

Note that because  $j$  itself is a subset of  $V_\lambda$ , the application operation so defined allows for the application of an embedding  $j$  in  $\mathcal{E}_\lambda$  to itself. Furthermore, by elementarity, the application operation is left distributive.

Rank-to-rank embeddings can be naturally extended to embeddings on subsets of  $V_\lambda$ , namely to  $\Sigma_0$ -embeddings  $j^+ : V_{\lambda+1} \rightarrow V_{\lambda+1}$ , through the application operation: Any  $j : V_\lambda \rightarrow V_\lambda$  uniquely determines a function  $j^+ : V_{\lambda+1} \rightarrow V_{\lambda+1}$  by

$$j^+(A) = \bigcup_{\alpha < \lambda} j(A \cap V_\alpha),$$

for  $A$  in  $V_{\lambda+1}$ . We call  $j^+$  *the extension of  $j$  to  $V_{\lambda+1}$* .

For embeddings  $j$  and  $k$  in  $\mathcal{E}_\lambda$ , we refer to  $j^+(k)$  as *application to  $k$  by  $j$*  and write  $jk = j \cdot k = j^+(k)$ .

## 2.2 Free Left Distributive Algebras

For any cardinal  $\kappa$ , one can form the free left distributive term algebra  $\mathcal{A}_\kappa$  on  $\kappa$  generators and one binary operation  $\cdot$  by forming all terms  $A_\kappa$  in the generators and  $\cdot$  and considering the algebra  $\mathcal{A}_\kappa$  of equivalence classes of those terms under the left distributive law (LD). Two terms  $u$  and  $v$  in  $\mathcal{A}_\kappa$  are LD-equivalent in  $\mathcal{A}_\kappa$  ( $u \equiv_{LD} v$ ) if and only if one can be obtained from the other by a series of applications of the left distributive law: namely,  $u$  can be obtained from  $v$  by a series of substitutions of the form  $a \cdot (b \cdot c) \leftrightarrow (a \cdot b) \cdot (a \cdot c)$ .

In the sequel we will follow convention and write  $\mathcal{E}_\lambda$  for the collection of all nontrivial elementary embeddings from  $V_\lambda$  to  $V_\lambda$ , where  $\lambda$  is a limit cardinal of cofinality  $\omega$ , and also  $ab$  for  $a \cdot b$  and  $a_1 a_2 a_3 \cdots a_{n-1} a_n$  for  $((((a_1 \cdot a_2) \cdot a_3) \cdots a_{n-1}) \cdot a_n)$ . Likewise we will write  $\mathcal{A} = \mathcal{A}_1$  for the free left distributive algebra on a single generator, and, for elementary embeddings  $j$  and  $k$  in  $\mathcal{E}_\lambda$ , we will write  $\mathcal{A}_j$

<sup>4</sup>Note that this equivalent to  $j$  extending to a  $\Sigma_n$ -elementary embedding  $V_{\lambda+1} \rightarrow V_{\lambda+1}$ .

<sup>5</sup> $L(V_{\lambda+1})$  is Gödel's constructible universe built on top of  $V_{\lambda+1}$ .

for  $\mathcal{A}_{\{j\}}$  and  $\mathcal{A}_{j,k}$  for  $\mathcal{A}_{\{j,k\}}$  (and refrain from using  $j$  and  $k$  as natural numbers in this context).

Laver gave the first nontrivial representation of a free left distributive algebra [15]. Specifically, he showed that the algebra of embeddings generated by closing a single nontrivial rank-to-rank elementary embedding  $j$  under the application operation (see subsection 2.1 for a definition) generates an algebra  $\mathcal{A}_j$  isomorphic to the free left distributive algebra  $\mathcal{A}$  [15]. To do so, he proved that the iterated left subterm relation  $<_L$  is a linear order of  $\mathcal{A}$  (where, for elements  $a$  and  $b$  of  $\mathcal{A}$ ,  $a <_L b$  means that there exist  $c_1, \dots, c_n$  in  $\mathcal{A}$  such that  $b = ac_1 \dots c_n$ ). He furthermore proved that  $\mathcal{A}_j \cong \mathcal{A}$  and that the word problem for  $\mathcal{A}$  is solvable: For every pair of words  $u$  and  $v$  in  $\mathcal{A}$ , exactly one of the following holds:  $u <_L v$ ,  $v <_L u$ , or  $u \equiv_{LD} v$ . Laver's result also gives that  $\mathcal{A}$  is left cancelative:  $ab <_L ac$  if and only if  $b <_L c$  and  $ab = ac$  if and only if  $b = c$ .

Laver obtained irreflexivity of  $<_L$  from the large cardinal assumption, using the fact that there do not exist rank-to-rank embeddings  $k, k_1, k_2, \dots, k_n$  in  $\mathcal{E}_\lambda$  such that  $k = kk_1 \dots k_n$ . Because the algebra of embeddings (and in particular  $\mathcal{A}_j$ ) is irreflexive, so too must be the free left distributive algebra. For connectedness ( $a \leq_L b$  or  $b \leq_L a$  for all  $a$  and  $b$  in  $\mathcal{A}_j$ ), he proved the existence of a normal form and a lexicographic ordering  $<_{Lex}$  on normal form terms that agrees with the left subterm relation  $<_L$  and the subterm relation  $<$ . That normal form takes place in a conservative extension  $\mathcal{P}$  of  $\mathcal{A}$ : For elements  $u$  and  $v$  of  $\mathcal{A}$  and  $R$  a relation in  $\{<_L, \equiv_{LD}, <_{Lex}, <\}$ , we have that  $uRv$  holds of  $u$  and  $v$  as elements of  $\mathcal{A}$  if and only if  $uRv$  holds of  $u$  and  $v$  as elements of  $\mathcal{P}$ .

Intuitively, the algebra  $\mathcal{P}$  is formed by freely adding a composition-like operation  $\circ$  to the application operation, so that  $\mathcal{P}$  satisfies the identities in  $\Sigma$  for all  $a, b$  and  $c$  in  $\mathcal{P}$ :

$$\Sigma = \{a \circ (b \circ c) = (a \circ b) \circ c, (a \circ b)c = a(bc), a(b \circ c) = ab \circ ac, a \circ b = ab \circ a\}.$$

The first two equations express that  $\circ$  is associative and behaves like composition when interacting with the application operation; the third asserts that left multiplication is still a homomorphism of the algebra; and the final law is now sometimes called the ‘‘braid law’’ in reference to the connection between left distributive algebras and Artin's braid group.<sup>6</sup>

For ease of reference, we summarize here several crucial results of Laver.

**Theorem 6** (Laver [15]). *The algebra  $\mathcal{P}$  is a conservative extension of  $\mathcal{A}$ : namely, if two terms in the language of  $\mathcal{A}$  can be proved equal using  $\Sigma$ , then they can be proved using just the left-distributive law. (See also [19].)*

**Theorem 7.** *Suppose there exists a nontrivial elementary embedding from  $V_\lambda \rightarrow V_\lambda$ .*

(a) *There exists a normal form for terms in  $\mathcal{A}$ , and  $<_{Lex}$ , the lexicographic ordering on normal form words is a linear ordering of  $\mathcal{A}$ .*

<sup>6</sup>In the braid groups, nonconsecutive generators  $\sigma_i$  and  $\sigma_j$  commute and consecutive ones satisfy  $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$ .

(b) The lexicographic ordering  $<_{Lex}$ , the iterated left subterm relation  $<_L$ , and the subterm relation  $<$  all agree<sup>7</sup>

**Corollary 8.** (a) The algebra  $\mathcal{A}_j$  formed by closing a single rank-to-rank embedding  $j$  under the binary application operation is isomorphic to the free left distributive algebra,  $\mathcal{A}$ ;

(b) The iterated left subterm relation  $<_L$  linearly orders  $\mathcal{A}$ ;

(c) The word problem for  $\mathcal{A}$  is solvable.

Laver later discovered another normal form called the division form that is more useful for applications [16]. It is used in the sequel, so we describe it here. The idea of the division form goes approximately like this. Suppose we have words  $a$  and  $b$  in  $\mathcal{A}$ , where  $a$  is an iterated left subterm of  $b$  ( $a <_L b$ ). Then find  $c_1$ , the  $<_L$ -greatest member of  $\mathcal{A}$  such that  $ac_1 \leq b$ . If we do not have equality, find the  $<_L$ -greatest word  $c_2$  such that both  $ac_1c_2 \leq_L b$  and  $c_2 \leq_L a$ . Continue in this manner until we have  $b = ac_1 \dots c_n$ , where, for each  $1 \leq i \leq n$ ,  $c_i \leq_L c_0c_1 \dots c_{i-2}$  (letting  $a = c_0$ ). The almost-descending condition is called *normality* and is defined below. The division form theorem [16] says that we can find a unique representation of this form for every  $u$  in  $\mathcal{A}$ , but the algorithm cannot be carried out in  $\mathcal{A}$ : we must go to  $\mathcal{P}$  to state and execute the division form algorithm. This is because  $\mathcal{A}$  does not contain the least upper bounds of all sequences of words in  $\mathcal{A}$ . For example, for  $a, b \in \mathcal{A}$ , the least upper bound of the sequence  $a, b, aba, aba(ab), aba(ab)(aba), \dots$  (called the iterates of  $a$  and  $b$ ) is  $a \circ b$ , which is not itself in  $\mathcal{A}$ .

Consider, for example, the term  $xx(xx)$ , where  $a = c_0 = x$ . Then  $c_1 = x$ , but  $c_2 = xx$  does not satisfy  $c_2 \leq_L c_0$ . Note that if we use  $a = xx$ , the term  $xx(xx)$  does satisfy the normality condition. This means that normality is a condition that depends on  $a$ , and we shall define  $a$ -normal below. Furthermore, normality is a property of literal terms in  $\mathcal{A}$  (respectively,  $P$ ,  $A_k$ , and  $P_k$ ), not on equivalence classes in  $\mathcal{A}$ .

Write  $a = a_0a_1 \dots a_{n-1} * a_n$  to denote a parsing of the term  $a$ , where  $*$  is either  $\cdot$  or  $\circ$ : In particular,  $a = a_0a_1 \dots a_{n-1} \cdot a_n$  or  $a = a_0a_1 \dots a_{n-1} \circ a_n$ .

To state the division form theorem more formally, we need a definition.

**Definition 9.** The representation of  $w = a_0a_1 \dots a_{n-1} * a_n$  in  $P$  is said to be  $a_0$ -normal with respect to the binary relation  $<_L$  if  $a_2 \leq_L a_0$ ,  $a_3 \leq_L a_0a_1$ , and  $a_i \leq_L a_0a_1 \dots a_{i-2}$  for all  $i$  such that  $2 \leq i \leq n$ , and if  $n \geq 2$  and  $* = \circ$ , then  $a_n <_L a_0a_1 \dots a_{n-2}$ .

The last condition of normality is to ensure the uniqueness of the representation by preventing applications of the braid law  $a \circ b = ab \circ a$ .

<sup>7</sup>In this paper we will actually use the *division form theorem* 12. The existence of the division form was first proven by Laver [16] as a consequence of the existence of the normal form; the result that all words in  $\mathcal{A}$  have a division form equivalent was later proven without relying on the normal form [15, Theorem 28], [20, 19].

**Definition 10** (Division Form). Define DF, the set of division form terms, to be the set of hereditarily  $x$ -normal terms in  $A$ . Namely,  $\text{DF} \subseteq P$  is the smallest set such that  $x$  is in DF and if  $a_1, \dots, a_n$  are in DF and  $w = xa_1 \cdots a_{n-1} * a_n$  is  $x$ -normal, then  $w$  is in DF. Write  $|w|$  for the division form of  $w$  and  $|w|^p$  for the  $p$ -division form of  $w$  (defined below).

**Definition 11** ( $p$ -Division Form). For any word  $p$  in  $\mathcal{P}$ , define  $p\text{-DF} \subseteq P$ , the set of  $p$ -division form terms, to be the smallest set such that:

- If  $w \leq_L p$  then  $w$  is in  $p\text{-DF}$  if and only if  $w$  is in DF, and
- If  $p <_L w$ ,  $w = |p|a_1a_2 \cdots a_{n-1} * a_n$ ,  $w$  is in  $p\text{-DF}$  if and only if  $w$  is  $p$ -normal,  $|p|$  is in DF and each  $a_i$  is in  $p\text{-DF}$ .

We can now state the division form theorem.

**Theorem 12** (Division Form Theorem (Laver [16])). *Every word in  $\mathcal{A}$  has a unique division form representation.*

The definitions of normality and of the division forms can be extended to the many generator case. (See [21] for definitions and related results.)

Through the connections between free LDAs and braid groups, Dehornoy was able to prove the solvability of the word problem for  $\mathcal{A}$  without the large cardinal hypothesis (at the expense of the normal form). Dehornoy worked in an extension of Artin's braid group on infinitely many generators  $B_\infty$  and defined a left distributive operation  $[\ ]$ . He then showed that a subset of  $B_\infty$  formed by closing a single element of  $B_\infty$  under the operation  $[\ ]$  gives rise to an algebra isomorphic to  $\mathcal{A}$  [6].

Importantly, he also proved more. In the case of free LDAs on more than one generator,  $<_L$  is no longer a linear ordering of  $\mathcal{A}_n$ . Say that  $u$  and  $v$  in  $\mathcal{A}_n$  have a *variable clash*, denoted  $u \approx v$ , if and only if there exist distinct variables  $x$  and  $y$  such that  $ax \leq_L u$  and  $ay \leq_L v$  for a (possibly empty) subterm  $a$  of  $u$  and  $v$ .

The confluence algorithm compares terms from  $\mathcal{A}$  by (repeated) substitution of subterms of the form  $u(vw)$  by those of the form  $uv(uw)$ . Dehornoy proved that the confluence algorithm terminates. In addition to resolving which of  $a <_L b$ ,  $b <_L a$ , and  $a \equiv_{LD} b$  hold in the one generator case of  $\mathcal{A}$ , confluence also gives information about the iterated left subterm relation  $<_L$  on free LDAs with more than one generator. Specifically, he proved that, for every natural number  $n$ ,  $\mathcal{A}_n$  is *confluent*. (See [5] and [7, Theorem 3.14]). This means that two terms  $a$  and  $b$  in  $\mathcal{A}_n$  are equivalent if and only if there exists a term  $c$  such that both  $a$  and  $b$  can be transformed into  $c$  using only forward applications of the left distributive law; namely, by replacing subwords of the form  $u(vw)$  with  $uv(uw)$ . Note that we can define  $\mathcal{P}_n$  analogously to  $\mathcal{P}$  by freely adding a composition operation  $\circ$  subject to the identities in  $\Sigma$  above.

In the sequel, we rely frequently on the following quadrichotomy theorem of Dehornoy, which is the best possible generalization of the linearity of  $<_L$  to LDAs with more than one generator.

**Theorem 13** (Dehornoy [7]). *For every natural number  $k$  and every pair  $u, v$  of elements of  $P_k$ , exactly one of the following holds:*

$$u = v, \quad u <_L v, \quad v <_L u, \quad u \approx v.$$

We now record some additional properties of LDAs that we will use in the sequel.

**Definition 14.** For any natural number  $n$  and any  $p$  in  $\mathcal{P}$ , define the  $n^{\text{th}}$  right power of  $p$ , denoted by  $p^{(n)}$ , recursively on  $n$  by

$$p^{(0)} = p \text{ and } p^{(n+1)} = p^{(n)}p^{(n)}.$$

We make extensive use of the fact that, for  $1 \leq i \leq n$ ,  $pp^{(n)} = p^{(n+1)} = p^{(i)}p^{(n)}$ , which holds for all  $n$  by a simple induction. For future reference, we isolate it here as Lemma 15.

**Lemma 15.** *For every  $p$  in  $\mathcal{P}$  and every natural number  $n$  and every  $i \leq n$ ,  $pp^{(n)} = p^{(i)}p^{(n)} = p^{(n)}p^{(n)} = p^{(n+1)}$ .*

The following proposition appears to be folklore. We record it for completeness, following the proof in [4, Theorem 3.14].

**Proposition 16.** *For all  $u$  and  $v$  in  $\mathcal{A}$ , there exist natural numbers  $n$  and  $m$  such that  $u^{(n)} = v^{(m)}$ .*

*Proof.* Let  $x$  be the generator of  $\mathcal{A} = \mathcal{A}_x$ . It suffices to show that for every  $u$  in  $\mathcal{A}$ , there are some  $n$  and  $m$  such that  $u^{(n)} = x^{(m)}$ .

We induct on the length of  $u$ . When the length is 1,  $u = x$  and we have  $u^{(0)} = u = x = x^{(0)}$ . Suppose the length of  $u$  is  $k+1 > 1$ . Then  $u = v \cdot w$  where the length of  $v$  and  $w$  are  $\leq k$ . Thus, there are  $n_v, n_w, m_v, m_w \in \omega$  such that  $v^{(n_v)} = x^{(m_v)}$  and  $w^{(n_w)} = x^{(m_w)}$ . Since  $(a^{(n)})^2 := a^{(n)}a^{(n)} = a^{(n+1)}$  for any  $a \in \mathcal{A}$ , by taking appropriate iterated squares of one of the equations, we may assume that  $m_v = m_w$ . We then compute

$$u^{(n_w)} = (vw)^{(n_w)} = v \cdot w^{(n_w)} = v \cdot x^{(m_w)} = v \cdot x^{(m_v)} = v \cdot v^{(n_v)} = v^{(n_v+1)} = x^{(m_v+1)}.$$

Thus, we have  $u^{(n)} = x^{(m)}$  for some  $n$  and  $m \in \omega$ , as desired.  $\square$

## 2.3 Square Roots

**Definition 17.** For  $k, j \in \mathcal{E}_\lambda$ , we say  $k$  is a *square root* of  $j$  if  $kk = j$ , and  $k$  is an  *$n$ -root* of  $j$  if  $k^{(n)} = j$ .

**Lemma 18.** *Suppose that  $j$  and  $k$  are in  $\mathcal{E}_\lambda$  and  $k$  is a square root of  $j$ . Then*

- (i) *The critical point of  $k$  is less than that of  $j$ :  $\text{crit } k < \text{crit } j$ , and*
- (ii) *For any  $a \in V_{\lambda+1}$ ,  $a \in \text{rng } k$  if and only if  $k(a) = j(a)$ .*

*Proof.* From the elementarity of  $k$  and the fact that  $kk = j$ , we have  $k(\text{crit } k) = \text{crit } (kk) = \text{crit } j$ ;  $k(\text{crit } k) > \text{crit } k$ , so the first claim holds. For the second part, let  $\bar{a}$  be such that  $k(\bar{a}) = a$ . Then  $j(a) = kk(a) = kk(k(\bar{a})) = k(k(\bar{a})) = k(a)$ . If  $k(a) = j(a)$ , then  $k(a) \in \text{rng } j = \text{rng}(kk)$ . So  $a \in \text{rng } k$ .  $\square$

**Theorem 19** (Laver [17, Theorem 13]). *If  $j \in \mathcal{E}_\lambda$ , then for any  $p$  and  $q$  in  $\mathcal{A}_j$ , if  $p \neq q$ , then  $p \upharpoonright \text{crit } \mathcal{A}_j \neq q \upharpoonright \text{crit } \mathcal{A}_j$ .*

Noting that for any  $n > 0$ , an  $n$ -root  $k$  of  $j$  is not in the algebra generated by  $j$ , we prove the following lemma.

**Lemma 20.** *If  $n < \omega$  and  $j, k \in \mathcal{E}_\lambda$  such that  $k^{(n)} = j$ . Then  $k \upharpoonright \mathcal{A}_j = j \upharpoonright \mathcal{A}_j$ .*

*Proof.* This follows immediately from Lemma 18 by induction on  $n$ . If  $n = 0$ , then  $k = j$ , so the conclusion clearly holds. Suppose  $n > 0$  and suppose that for any  $l \leq n$  and  $j, k \in \mathcal{E}_\lambda$  such that  $k^{(l)} = j$ , we have  $k \upharpoonright \mathcal{A}_j = j \upharpoonright \mathcal{A}_j$ . Let  $j, k \in \mathcal{E}_\lambda$  be such that  $k^{(n+1)} = j$ . Note that  $k^{(n)}k^{(n)} = k^{(n+1)}$ . Apply Lemma 18 to  $k^{(n)}, k^{(n+1)}$ , using the fact that  $\mathcal{A}_j \subseteq \text{rng } k^{(n)}$ , we have that  $k^{(n)} \upharpoonright \mathcal{A}_j = k^{(n+1)} \upharpoonright \mathcal{A}_j = j \upharpoonright \mathcal{A}_j$ . Now we apply the induction hypothesis to  $k, k^{(n)}$  to get  $k \upharpoonright \mathcal{A}_j = k^{(n)} \upharpoonright \mathcal{A}_j$ .<sup>8</sup> Therefore  $k \upharpoonright \mathcal{A}_j = j \upharpoonright \mathcal{A}_j$  as desired.  $\square$

### 3 Pulling back in the algebra

For the main results of this paper, proven in Sections 4 and 5, we make frequent use of the properties of the range function, including when we can sensically discuss the preimage—called a *pullback*—of one embedding under another. The pullback of one embedding by another is itself an elementary embedding, but that embedding is not *a priori* in  $\mathcal{A}_j$ , even when both embeddings are. In this section, we provide basic definitions and prove properties of pullbacks.

We are interested in the conditions under which the pullback of one embedding by another is certain to (exist as an embedding and) be contained in a given algebra, such as  $\mathcal{A}_j$ . Theorem 27 of this section relates pairs of elements to the conditions under which their pullbacks are elements of  $\mathcal{A}_j$ . We furthermore conjecture that Theorem 27 can be extended to finitely generated algebras of embeddings in Conjecture 28.

**Definition 21.** For  $j, k \in \mathcal{E}_\lambda$ , by the *pullback* of  $k$  by  $j$ , we mean  $(j^+)^{-1}(k)$ . Recall that  $j^+$  denotes the extension of  $j$  in  $\mathcal{E}_\lambda$  to a function  $j^+$  from  $V_{\lambda+1}$  to  $V_{\lambda+1}$ . For brevity, we will write  $j^{-1}(k)$  for the pullback of  $k$  by  $j$ .

**Lemma 22.** *For embeddings  $j, k \in \mathcal{E}_\lambda$ , if  $n < \omega$  and  $j$  and  $jk$  are both  $\Sigma_n^1$ -elementary, then  $k = j^{-1}(jk) \in \mathcal{E}_\lambda$  (the pullback of  $jk$  by  $j$ ) is  $\Sigma_n^1$ -elementary.*

*Proof.* The proof is very similar to the proof of Theorem 2.4 of [18].  $\square$

**Lemma 23.** *For embeddings  $j$  and  $k$  in  $\mathcal{E}_\lambda$ ,*

$$j \in \text{rng } k^+ \Leftrightarrow kj = kkj.$$

<sup>8</sup>Note that  $\mathcal{A}_j \subseteq \mathcal{A}_{k^{(n)}}$ .

**Remark 24.** For brevity, we will not write the “+” in the following proofs.

*Proof.* By the hypothesis that  $j$  is in the range of  $k$ , there is some  $\bar{j} \in \mathcal{E}_\lambda$ . Observe that  $j = k\bar{j}$ , then  $kj = k(k\bar{j}) = kk(k\bar{j}) = kkj$ , where the second equality follows from left distributivity.

For the other direction, suppose  $kj = kkj$ . Then  $kkj$  is the image of  $j$  under  $k$  and thus in the range of  $k$ . Since both  $kkj$  and  $kk$  are in the range of  $k$ , the pullback of  $kkj$  by  $kk$ ,  $(kk)^{-1}(kkj) = j$  (being  $\Sigma_0$ -definable from these embeddings), is in the range of  $k$  by elementarity, as desired.  $\square$

**Definition 25.** For elements  $a$  and  $b$  of  $\mathcal{A}$  (respectively,  $\mathcal{P}$ ), we say that  $a$  *divides*  $b$ , denoted by  $a|b$ , if and only if there exists  $c$  in  $\mathcal{A}$  (respectively,  $\mathcal{P}$ ) such that  $b = ac$ .

**Lemma 26.** For  $a, b \in \mathcal{P}$ ,  $a$  divides  $b$  (in  $\mathcal{P}$ ) if and only if  $ab = aab$ . Similarly if  $a, b \in \mathcal{A}$ ,  $a$  divides  $b$  (in  $\mathcal{A}$ ) if and only if  $ab = aab$ .

*Proof.* The forward direction follows directly from Lemma 23: If  $a$  divides  $b$ , then  $b = ac$  for some  $c$  in  $\mathcal{P}$ . Then  $ab = a(ac) = aa(ac) = aab$ .

For the backward direction, suppose that  $ab = aab$ . We first prove that this entails  $a <_L b$ . Equality of  $a$  and  $b$  is impossible by irreflexivity of elementary embeddings (else  $aa = aaa$ ), so suppose for sake of contradiction that  $b <_L a$  holds. Then, there exist  $a_1, \dots, a_n$  in  $\mathcal{P}$  such that  $a = ba_1a_2 \cdots a_{n-1} * a_n$ , where  $*$  is either  $\cdot$  or  $\circ$ . But then

$$ab = aab = a(ba_1 \cdots a_{n-1} * a_n)b = ((ab)(aa_1) \cdots (aa_{n-1}) * (aa_n))b.$$

The right hand side is  $(ab)(aa_1) \cdots (aa_{n-1})(aa_n)b$  when  $*$  is  $\cdot$  and

$$((ab)(aa_1) \cdots (aa_{n-1}) \circ (aa_n))b = (ab)(aa_1) \cdots (aa_{n-1})(aa_nb)$$

when  $*$  is  $\circ$ . Both possibilities contradict the irreflexivity of  $<_L$ .

Assume therefore that  $b >_L a$ . Let  $b = ab_1b_2 \cdots b_{n-1} * b_n$  be the  $|a|$ -division form of  $b$ . We compute:

$$ab = a(ab_1b_2 \cdots b_{n-1} * b_n) = aa(ab_1)(ab_2) \cdots (ab_{n-1}) * (ab_n),$$

$$aab = aa(ab_1b_2 \cdots b_{n-1} * b_n) = aa(ab_1)(aab_2) \cdots (aab_{n-1}) * (aab_n).$$

We claim that both of these are  $aa(ab_1)$ -normal, and thus in  $|aa(ab_1)|$ -division form once the individual components are in  $aa(ab_1)$ -division form. We need to show that  $ab_i \leq_L aa(ab_1) \cdots (ab_{i-2})$  for  $2 < i \leq n$ , with strict inequality if  $*$  is  $\circ$  and  $i = n$ . Because  $\mathcal{A}$  is left cancelative, multiplying the inequality  $b_i \leq_L ab_1 \cdots b_{i-2}$  on the left by  $a$  preserves the inequality, including in the case where  $i = n$  and  $*$  is  $\circ$ , so the inequality is strict. Similarly, applying  $aa$  to these inequalities shows us that the second word is also in  $|aa(ab_1)|$ -normal. The two words therefore have the same  $|aa(ab_1)|$ -division forms and thus must be identical. In particular, we have  $ab_2 = aab_2$  if  $n \geq 2$ .

If  $n \geq 2$ , then the assumption that  $ab_1 \cdots b_{n-1} * b_n$  is the  $|a|$ -division form of  $b$  gives that  $b_2 \leq_L a$ . The same argument showing that  $a <_L b$  shows that  $ab_2 <_L aab_2$ . Therefore, we have both that  $ab_2 = aab_2$  and that  $ab_2 <_L aab_2$ , contradicting the linearity of  $<_L$  (see Theorem 7).

The only remaining case is  $n = 1$  and  $b = ab_1$ ; this proves that  $a|b$ , as desired.

To see that the corresponding statement holds in  $\mathcal{A}$ , note that if  $a$  and  $b$  are in  $\mathcal{A}$  and  $a$  divides  $b$  in  $\mathcal{P}$ , then  $a$  divides  $b$  in  $\mathcal{A}$ . In particular,  $a|b$  if and only if there exists a  $c$  in  $\mathcal{P}$  such that  $b = ac$ , but because  $b$  is in  $\mathcal{A}$ ,  $c$  must also be in  $\mathcal{A}$  (otherwise, it would contain an essential composition and  $b$  would be in  $\mathcal{P} \setminus \mathcal{A}$ —see [19, page 2158]).  $\square$

We are now ready to prove the following theorem.

**Theorem 27.** *Let  $j$  be an elementary embedding in  $\mathcal{E}_\lambda$ . For elements  $\ell$  and  $p$  in  $\mathcal{A}_j$ , the following are equivalent.*

1. *The pullback of  $p$  by  $\ell$ ,  $\ell^{-1}p$ , exists as an embedding in  $\mathcal{E}_\lambda$ .*
2. *The pullback of  $p$  by  $\ell$ ,  $\ell^{-1}p$ , is an embedding in  $\mathcal{A}_j$ .*
3. *The word  $\ell$  divides  $p$  as an element of the algebra  $\mathcal{A}_j$ .*

*Proof.* (2) implies (1) since  $\mathcal{A}_j \subset \mathcal{E}_\lambda$ .

(1) implies (3): Let  $q = \ell^{-1}p \in \mathcal{E}_\lambda$ , so that  $\ell q = p$ . Thus,

$$\ell p = \ell(\ell q) = (\ell\ell)(\ell q) = \ell\ell p.$$

By Lemma 26, we have  $\ell$  divides  $p$  in  $\mathcal{A}_j$ .

(3) implies (2) is the definition of divisibility.  $\square$

(1) implies (2) of Theorem 27 is the  $n = 1$  case of the following conjecture.

**Conjecture 28.** *Suppose  $k_1, \dots, k_n$  are elementary embeddings in  $\mathcal{E}_\lambda$  such that  $\mathcal{A}_{k_1, \dots, k_n}$  is free and that  $\ell, p \in \mathcal{A}_{k_1, \dots, k_n}$ . If  $\ell^{-1}p$  exists, then  $\ell^{-1}p \in \mathcal{A}_{k_1, \dots, k_n}$ .*

## 4 Elementary Equivalence and Finitely Generated Free LDAs

One of the first insights gained from manipulating terms in the one- and many-generated free LDAs is that they are qualitatively different due to the existence of variable clashes in the multivariable cases. In this section, we analyze that experiential difference using elementary equivalence. The main result of this section, Theorem 36, says that all finitely-generated free LDAs are  $\Sigma_1$ -elementarily equivalent but not  $\Sigma_2$ -elementarily equivalent. Our proof of  $\Sigma_1$ -elementary equivalence uses large cardinals in an essential way; whether a ZFC proof exists is an open question. The non- $\Sigma_2$ -elementary equivalence, however, is provable in ZF. This non-equivalence at the level of  $\Sigma_2$  is in contrast with

two famous examples from group theory. The first is Tarski's famous conjecture [23], that all free groups (with more than one generator) are elementarily equivalent. Free abelian groups are  $\Sigma_2$ -elementarily equivalent but not  $\Sigma_3$ -elementarily equivalent.

In general, square roots of elementary embeddings have weaker elementarity properties than the embeddings from which they are derived. In order to prove Theorem 36, we must first establish a series of lemmas guaranteeing that we can generate the sequences of square roots of embeddings we will need.

The version of Lemma 29 presented here is a slight extension of the construction implicit in [18, Lemma 2.2], as proven in [1].

**Lemma 29.** *Suppose  $j \in \mathcal{E}_\lambda$ . Then the following are equivalent.*

1. *The embedding  $j$  is  $\Sigma_1$ -elementary.*
2. *For any  $c_0, \dots, c_s \in V_{\lambda+1}$  there is  $k \in \mathcal{E}_\lambda$  that is a square root of  $j$  such that  $c_0, \dots, c_s \in \text{rng } k$ .*
3. *For any  $a_0, \dots, a_m, b_0, \dots, b_n \in V_{\lambda+1}$  there is  $k \in \mathcal{E}_\lambda$  such that  $a_0, \dots, a_m \in \text{rng } k$  and for all  $\ell \leq n$ ,  $k(b_\ell) = j(b_\ell)$ .*

*Proof.* For (1) implies (2), see [1, Lemma 16]. (2) implying (3) follows Lemma 18.

For (3) implies (1), suppose that

$$V_{\lambda+1} \models \exists y_0, \dots, y_m \phi[c_0, \dots, c_n, y_0, \dots, y_m],$$

where  $\phi$  is  $\Sigma_0$  and  $c_0, \dots, c_n$  in the range of  $j$  with preimages  $b_0, \dots, b_n$ , and suppose  $a_0, \dots, a_m$  witness this statement. Then there exists a  $k$  such that  $a_0, \dots, a_m \in \text{rng } k$  and  $k(b_i) = j(b_i)$  for  $i < n$ . Let  $\bar{a}_0, \dots, \bar{a}_m$  be the preimages of  $a_0, \dots, a_m$  under  $k$ . We have that

$$\begin{aligned} V_{\lambda+1} \models \phi[c_0, \dots, c_n, a_0, \dots, a_m] &\Rightarrow V_{\lambda+1} \models \phi[b_0, \dots, b_n, \bar{a}_0, \dots, \bar{a}_m] \\ &\Rightarrow V_{\lambda+1} \models \exists y_0, \dots, y_m \phi[b_0, \dots, b_n, y_0, \dots, y_m] \end{aligned}$$

So we have the desired result.  $\square$

A similar argument to the previous gives the following:

**Lemma 30.** *For  $n \geq 1$ ,  $j : V_{\lambda+1} \rightarrow V_{\lambda+1}$  is a  $\Sigma_{2n+1}$  elementary map if and only if for every  $a_0, \dots, a_m, b_0, \dots, b_n \in V_{\lambda+1}$ , there is some  $\Sigma_{2n-1}$  elementary map  $k : V_{\lambda+1} \rightarrow V_{\lambda+1}$  which is a square root of  $j$  such that  $a_0, \dots, a_m \in \text{rng } k$  and for all  $\ell \leq n$ ,  $k(b_\ell) = j(b_\ell)$ .*

The nature of the strength hypotheses in the previous two lemmas is clarified by the following result of Martin.

**Lemma 31 (Martin).** *If  $j : V_{\lambda+1} \rightarrow V_{\lambda+1}$  is  $\Sigma_{2n-1}$ -elementary for  $n \geq 1$ , then  $j$  is  $\Sigma_{2n}$ -elementary.*

Given the previous lemmas, we make the following definition.

**Definition 32.** Define  $\mathcal{E}_\lambda^n$  to be the set of nontrivial  $j : V_\lambda \rightarrow V_\lambda$  that can be extended to  $\Sigma_n$ -elementary embeddings  $j^+ : V_{\lambda+1} \rightarrow V_{\lambda+1}$ .

In light of Martin's Lemma (Lemma 31) and Lemma 30, we will talk only about embeddings in  $\mathcal{E}_\lambda^{2^n}$ .

We can then rephrase Lemmas 29 and 30 as the following.

**Lemma 33.**  $j \in \mathcal{E}_\lambda^{2^{n+1}}$  if and only if for every  $a_0, \dots, a_m, b_0, \dots, b_n \in V_{\lambda+1}$ , there is some  $k \in \mathcal{E}_\lambda^{2^n}$  a square root of  $j$  such that  $a_0, \dots, a_m \in \text{rng } k$  and for all  $\ell \leq n$ ,  $k(b_\ell) = j(b_\ell)$ .

Lemma 33 allows us to produce arbitrarily long finite sequences of iterated square roots of  $j$  when  $j^+$  is a fully elementary embedding  $j^+ : V_{\lambda+1} \rightarrow V_{\lambda+1}$ . Lemma 18 and well-foundedness, however, prevent an infinite sequence of such square roots.

**Lemma 34.** Suppose  $j \in \mathcal{E}_\lambda$  and  $j^+ : V_{\lambda+1} \rightarrow V_{\lambda+1}$  is fully elementary. Then for any  $p, q < \omega$  and for any  $a_0, \dots, a_m, b_0, \dots, b_n \in V_{\lambda+1}$ , there is a sequence of embeddings  $k_i \in \mathcal{E}_\lambda^{2^{(i+q)}}$  for  $i \leq p$  such that:

1.  $k_p$  is a square root of  $j$ ;
2. For all  $i < p$ ,  $k_i$  is a square root of  $k_{i+1}$ ;
3. For all  $i \leq p$ ,  $a_0, \dots, a_m$  are in the range of  $k_i$  and for all  $\ell \leq n$ , the  $k_i$  agree with  $j$  on the  $b_\ell$ :  $k_i(b_\ell) = j(b_\ell)$ ; and
4. Each of  $a_0, \dots, a_m$  are in the range of  $k_p \circ k_{p-1} \circ \dots \circ k_0$ .

*Proof.* We simply apply Lemma 33  $p+1$  many times to  $a_0, \dots, a_m, b_0, \dots, b_n$  in the natural way to obtain the sequence of embeddings  $k_p, k_{p-1}, \dots, k_1, k_0$ , with  $k_p$  a square root of  $j$ ,  $k_{p-1}$  square root of  $k_p$ , etc. It is clear from this process that properties (1)-(3) hold. To see that (4) holds, note, for instance, that  $a_0 \in \text{rng } k_p$ . Since  $k_{p-1}$  is a square root of  $k_p$ , so  $k_p \in \text{rng } k_{p-1}$ , and  $a_0 \in \text{rng } k_{p-1}$ , we have that  $k_p^{-1}(a_0) \in \text{rng } k_{p-1}$ . Hence  $a_0$  is in the range of  $k_p \circ k_{p-1}$ . Similarly, by induction,  $a_0 \in \text{rng } k_p \circ \dots \circ k_0$ . Thus (4) clearly follows.  $\square$

The proof of Theorem 36 uses the following Theorem of Laver-Steel.

**Theorem 35** (Laver-Steel [17]). *Let  $j \in \mathcal{E}_\lambda$ . Then  $\text{crit } \mathcal{A}_j$  has order type  $\omega$ .*

We are now ready to prove the theorem. In part (1) of the theorem, the Large Cardinal (LC) assumption is precisely the existence of a nontrivial elementary embedding  $V_{\lambda+1} \rightarrow V_{\lambda+1}$ .

**Theorem 36.** 1. (LC) *Assume that there exists a nontrivial elementary embedding  $V_{\lambda+1} \rightarrow V_{\lambda+1}$ , then  $\mathcal{A}_n \equiv_1 \mathcal{A}_m$  for all  $n, m \leq \omega$ .*

2. (ZF)  $\mathcal{A}_n \not\equiv_2 \mathcal{A}_m$  for all  $n \neq m \leq \omega$ .

*Proof.* For (1), we first show  $\mathcal{A}_2 \equiv_1 \mathcal{A}_1$ . Since  $\mathcal{A}_1$  can be naturally embedded into  $\mathcal{A}_2$ , it suffices to show that any  $\Sigma_1$ -statement true in  $\mathcal{A}_2$  is also true in  $\mathcal{A}_1$ .

Let  $j \in \mathcal{E}_{\lambda+1}$ . Following [1], we consider the embeddings  $k$  and  $\ell$  defined by  $k = j \circ j^{(1)} \circ j^{(2)} \circ \dots$  and  $\ell = j \circ j \circ j^{(1)} \circ j^{(2)} \circ \dots$ . By [1],  $k, \ell \in \mathcal{E}_\lambda$  and  $\mathcal{A}_{k,\ell}$  is a free, 2-generated LDA.

Suppose  $\mathcal{A}_{k,\ell} \models \exists \bar{x} \varphi'(\bar{x})$  where  $\varphi'(\bar{x})$  is quantifier-free. Since  $\mathcal{A}_{k,\ell}$  is generated by  $k$  and  $\ell$ , we can replace the witness of  $\varphi'$  by terms in  $k$  and  $\ell$ , so we may assume that  $\mathcal{A}_{k,\ell} \models \varphi(k, \ell)$  where  $\varphi$  is quantifier-free. It suffices to show that  $\mathcal{A}_1 \models \exists k^* \exists \ell^* \varphi(k^*, \ell^*)$ . We may assume that

$$\varphi(x, y) = \bigwedge_i s_i(x, y) \neq t_i(x, y) \wedge \bigwedge_i s'_i(x, y) = t'_i(x, y)$$

where  $s_i(x, y), t_i(x, y), s'_i(x, y), t'_i(x, y)$  are terms in the language of LDAs involving  $x, y$ .

We define for  $n < \omega$ ,  $k_n = j \circ j^{(1)} \circ j^{(2)} \circ \dots \circ j^{(n)}$  and  $\ell_n = j \circ j \circ j^{(1)} \circ j^{(2)} \circ \dots \circ j^{(n)}$ . Let  $\langle \delta_n \mid n < \omega \rangle$  be the increasing enumeration of  $\text{crit } \mathcal{A}_j$ . We have that for any  $n < \omega$ ,  $k_n \upharpoonright V_{\delta_n} = k \upharpoonright V_{\delta_n}$ , and  $\ell_n \upharpoonright V_{\delta_n} = \ell \upharpoonright V_{\delta_n}$ , since  $\delta_n \leq \text{crit } j^{(n)}$ .

Assume  $n$  is large enough so that, for all the (finitely many)  $i$ 's in  $\varphi$

$$s_i(k_n, \ell_n) \upharpoonright V_{\delta_n} \neq t_i(k_n, \ell_n) \upharpoonright V_{\delta_n}.$$

By Theorem 10 of [17] there are embeddings  $k^*$  and  $\ell^*$  in  $\mathcal{A}_j$  such that

$$k^* \upharpoonright V_{\delta_n} = k_n \upharpoonright V_{\delta_n}$$

and

$$\ell^* \upharpoonright V_{\delta_n} = \ell_n \upharpoonright V_{\delta_n}.$$

We then have that for all  $i$ ,

$$s_i(k^*, \ell^*) \neq t_i(k^*, \ell^*).$$

Recall that, in an equational class (in the sense of universal algebra), any positive atomic formula true about the generators of a free structure is true about any tuple in any structure in the class [3, Theorem 11.4]. In our setting, since  $k$  and  $\ell$  are free generators of  $\mathcal{A}_{k,\ell} \cong \mathcal{A}_2$ , any two elements of any LDA will satisfy any equations that  $k$  and  $\ell$  satisfy. In particular, since  $s'_i(k, \ell) = t'_i(k, \ell)$ , we have that  $s'_i(k^*, \ell^*) = t'_i(k^*, \ell^*)$ . So  $k^*$  and  $\ell^*$  satisfy  $\varphi$ , namely,

$$\mathcal{A}_1 \models \varphi(k^*, \ell^*)$$

as desired.

We now consider the other case of (1) and show that  $\mathcal{A}_n \equiv_1 \mathcal{A}_m$  for  $n, m \geq 2$ . It suffices to prove that  $\mathcal{A}_3$  embeds into  $\mathcal{A}_2$ , then proceeds by induction. By Brooke-Taylor-Cramer-Miller-Edwards [1], we can find  $k, \ell$  with disjoint iterated

ranges. By Lemma 30, there are some elementary embeddings  $j$  and  $\bar{\ell}$  such that  $k = \bar{\ell}j$  and  $\ell = \bar{\ell}\bar{\ell}$ . Then  $\langle j, k, \ell \rangle = \langle j, \bar{\ell}j, \bar{\ell}\bar{\ell} \rangle \subseteq \langle j, \bar{\ell} \rangle$ . We show that  $\langle j, k, \ell \rangle$  is free. This follows since  $\text{irng } k, \text{irng } \ell \subseteq \text{irng } \bar{\ell}$ . So since  $\text{irng } \bar{\ell}$  and  $\text{irng } j$  are disjoint (by elementarity of  $\bar{\ell}$  and the fact that  $\text{irng } k$  and  $\text{irng } \ell$  are disjoint), this implies that  $\text{irng } k$  and  $\text{irng } \ell$  are disjoint from  $\text{irng } j$ .

Since  $\text{irng } j$  and  $\text{irng } \bar{\ell}$  are disjoint,  $\langle j, \bar{\ell} \rangle$  is also free. Hence we have that since  $\langle j, k, \ell \rangle$  embeds into  $\langle j, \bar{\ell} \rangle$ , that  $\mathcal{A}_3$  embeds into  $\mathcal{A}_2$ .

To show (2), notice first that the set of standard generators is definable via the universal formula:  $\psi(x) = \forall y, z, x \neq y \cdot z$ . Thus, saying the rank of  $\mathcal{A}_n$  is at least  $n$  is  $\Sigma_2$  by the sentence  $\varphi_n \equiv \exists x_1, \dots, x_n \left( \bigwedge_{i \neq j} x_i \neq x_j \wedge \bigwedge_{1 \leq i \leq n} \psi(x_i) \right)$ . So if  $n > m$ , then  $\mathcal{A}_n \models \varphi_n$  but  $\mathcal{A}_m \models \neg \varphi_n$ . This shows  $\mathcal{A}_n \not\equiv_2 \mathcal{A}_m$ .  $\square$

## 5 Capturing the Algebraic Structure of Elementary Embeddings

One of our primary motivating questions is whether algebras of rank-into-rank elementary embeddings always embed into simply definable left distributive algebras. Laver answered this question in the affirmative for algebras with a single generator.

We pose this general motivating question as follows.

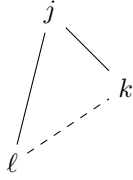
**Question 37.** *Is there a simply definable algebra which embeds  $\langle E \rangle$  for any countable  $E \subseteq \mathcal{E}_\lambda$ ?*

A natural next step beyond the Laver-Steel Theorem would be to consider two rank-to-rank elementary embeddings; namely, given rank-to-rank embeddings  $k$  and  $\ell$ , does  $\mathcal{A}_{k,\ell} = \langle k, \ell \rangle$ , the algebra generated by closing  $k$  and  $\ell$  under application and forming equivalence classes under the left distributive law, embed into a simply definable algebra?

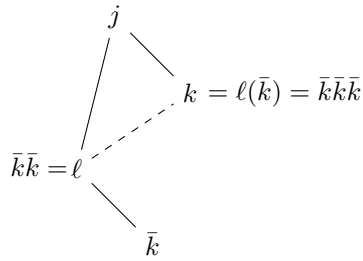
With certain additional assumptions on our embeddings, we can answer this question in the affirmative. As a warm-up, we describe the idea for proving the following Proposition which is a special case of Corollary 45 below.

**Proposition 38.** *Suppose that  $k_0, \dots, k_n$  are square roots of  $j \in \mathcal{E}_\lambda$  such that for all  $m < i \leq n$ ,  $k_i \in \text{rng } k_m$ . Then  $\langle k_0, \dots, k_n \rangle$  embeds into  $\mathcal{A}_1$ .*

*Proof sketch.* Suppose first that  $k$  and  $\ell$  are both square roots of an embedding  $j$  and that  $k$  is in the range of  $\ell$ . We represent this in the diagram below, where solid lines indicate that the embedding lower in the diagram is a square root of the embedding above it, and dashed lines mean that the lower embedding has the higher embedding in its range.

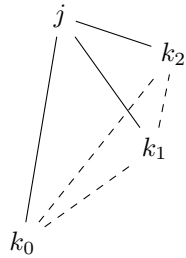


For  $k$  and  $\ell$  as above, we can show that  $\langle k, \ell \rangle$  embeds into  $\mathcal{A}$ . This is because  $\bar{k} = \ell^{-1}(k)$  generates both  $k$  and  $\ell$ :  $\bar{k}$  is a square root of  $\ell$  since we can pull back the fact that  $k$  is a square root of  $j$  by  $\ell$ . We can show this in a diagram as follows:

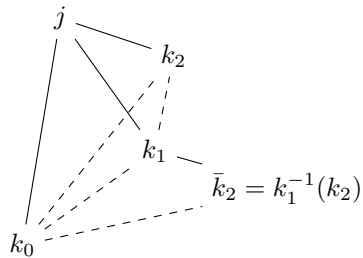


But  $\ell(\bar{k}) = k$ , so we have that  $\langle k, \ell \rangle$  is a subset of  $\mathcal{A}_{\bar{k}} \cong \mathcal{A}$ .

This argument generalizes to the general case. We illustrate this for  $n = 2$  in the following diagram:



Pulling back  $k_2$  by  $k_1$  we get the following:





2. Note that if  $S$  is finite and square-full, then  $S$  must be square-confluent as well, as there must be a top element. We will use this fact largely without mention below.
3. Note that any subset of a rigid set is also rigid.

For the next lemma, we define the *right depth*  $r(t)$  for a term  $t$  representing some word in  $\mathcal{A} = \mathcal{A}_x$  recursively by  $r(x) = 1$  and  $r(t) = r(v) + 1$  if  $t = uv$ . Dehornoy [7] showed that this is well-defined on  $\mathcal{A}$ , namely, if  $t$  and  $t'$  represent the same word in  $\mathcal{A}$ , then  $r(t) = r(t')$ .

**Lemma 41.** *Let  $a$  be in  $\mathcal{A}$  with  $a \neq x$  and suppose there exist  $m, n < \omega$  such that  $a$  is an  $m^{\text{th}}$  root of  $x^{(n)}$ , namely,  $a^{(m)} = x^{(n)}$ . Then  $m < n$ .*

*Proof.* Note that  $r(a^{(m)}) = r(a) + m$ , and that  $r(a) \geq 2$  if  $a \neq x$ . Thus, from  $a^{(m)} = x^{(n)}$ , we have  $m + r(a) = n + 1$ , so we have  $m < n$ .  $\square$

**Lemma 42.** *If  $S$  is rigid, weakly square-full, and finite and  $S = \{k_0, k_1, \dots, k_n\}$  such that for  $i < j$ ,  $k_i \in \text{rng } k_j$ , then*

1.  $k_1$  is a square root of  $k_0$ ,
2. For all  $1 \leq i \leq n$ ,  $k_i$  is an  $m$ th root of  $k_0$  for some  $m \leq i$ .

*Proof.* Note that (1) is a special case of (2), and is the base case of the induction to prove (2). To see (1) by definition of weakly square-full we have  $k_1 k_1 \in \mathcal{A}_{k_0}$ . But if  $k_1 k_1$  is not  $k_0$  then it must be an iterated square root of  $k_0$  which is not possible. So it must be  $k_0$ .

We prove (2) by induction on  $i$ . We want to show that  $k_i k_i$  is an  $m$ th root of  $k_0$  for some  $m \leq i$ . We have  $k_i k_i \in \mathcal{A}_{k_p}$  for some  $p < i$ . Since  $k_p$  is an  $m'$ th root of  $k_0$  for some  $m' \leq p$ , using Lemma 41 on  $\mathcal{A}_{k_p}$  and considering  $k_0 = k_p^{(m')}$  and  $k_i k_i$  as an iterated root of  $k_0$ ,  $k_i k_i$  is an  $m''$ th root of  $k_0$  for some  $m'' \leq m' \leq p < i$  (the equality holding if  $k_p = k_i k_i$ ). So we are done.  $\square$

**Lemma 43.** *Suppose  $m < \omega$  and  $S \subseteq \mathcal{E}_\lambda^m$  is a set of elementary embeddings such that  $S$  is finite, rigid, and weakly square-full. Write  $S = \{k_0, k_1, \dots, k_n\}$  such that for  $i < j$ ,  $k_i \in \text{rng } k_j$ .*

*Then  $S \subseteq \mathcal{A}_\ell$  for*

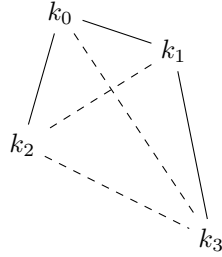
$$\ell = (k_1 \circ k_2 \circ \dots \circ k_n)^{-1}(k_0).$$

*Also  $\ell \in \mathcal{E}_\lambda^m$  is an  $n$ th root of  $k_0$  for  $n = |S| - 1$ .*

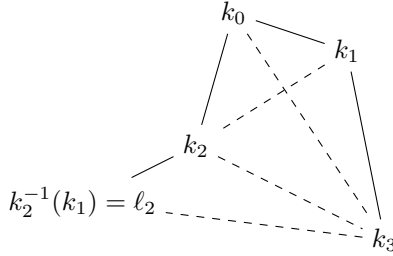
In this case, we say that the  $\ell$  is the *natural pullback given by  $S$* . By the proof of part (4) in Lemma 34, the natural pullback given by  $S$  always exists for sets  $S$  that are finite and rigid.

**Definition 44.** Suppose  $S \subseteq \mathcal{E}_\lambda$  is nonempty, finite, and rigid. Write  $S = \{k_0, k_1, \dots, k_n\}$  such that for  $i < j$ ,  $k_i \in \text{rng } k_j$ . We define the *natural pullback of  $S$*  to be  $(k_1 \circ k_2 \circ \dots \circ k_n)^{-1}(k_0)$ .

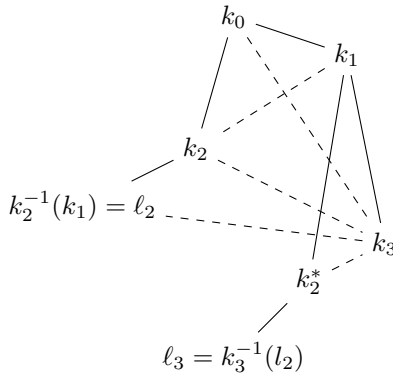
The proof of this lemma is a natural generalization of the ‘diagram arguments’ presented above. To give the reader intuition about how this situation differs, we provide the diagrams for the case that  $k_1k_1 = k_0$ ,  $k_2k_2 = k_0$ , and  $k_3k_3 = k_1$ . The diagram of  $S = \{k_0, k_1, k_2, k_3\}$  then looks as follows:



We step by step compute  $(k_1 \circ k_2 \circ k_3)^{-1}(k_0)$  and call the sequence of embeddings  $\ell_1, \ell_2, \ell_3$ . Pulling back  $k_0$  by  $k_1$  gives  $\ell_1 = k_1$  itself. Pulling this back by  $k_2$  we obtain the following:



Pulling back  $\ell_2$  by  $k_3$  we obtain:



Note that  $\langle \ell_2, k_2, k_0, k_1 \rangle \cong \langle \ell_3, k_2^*, k_1, k_3 \rangle$  because the right embeddings are pullbacks of the left embeddings by  $k_3$ . This implies the structure of the above diagram. So, retracing our steps, we can check that this entire diagram exists in  $\mathcal{A}_{\ell_3}$ , as desired.

*Proof of Lemma 43.* Write  $S = \{k_0, k_1, \dots, k_n\}$  such that for  $i < j$ ,  $k_i \in \text{rng } k_j$ .

By inducting on  $i$ , we will prove that  $k_0, \dots, k_i$  are generated by  $(k_1 \circ k_2 \circ \dots \circ k_i)^{-1}(k_0) = \ell_i$  and  $\ell_i$  is an  $n$ th root of  $k_0$  for some  $n$ . For the base case, we need to see that letting  $l_1 = k_1^{-1}(k_0)$ , then  $\{k_0, k_1\} \subseteq \mathcal{A}_{l_1}$ . By weak square-fullness of  $S$  and the way elements of  $S$  are enumerated, it follows from Theorem 42 that  $k_1 k_1 = k_0$ , so  $k_1^{-1}(k_0) = k_1$ ; therefore,  $k_1 = l_1$  and  $\{k_0, k_1\} \subseteq \mathcal{A}_{l_1}$ .

Assuming it is true for  $i$ , we prove it for  $i+1$ . So  $k_0, \dots, k_i$  are generated by  $\ell_i$ . We have  $\ell_{i+1} = k_{i+1}^{-1}(\ell_i)$ . We have that  $k_{i+1} k_{i+1} \in \mathcal{A}_{k_s}$  for some  $s \leq i$  by weak square-fullness. Hence by elementarity since  $k_s$  is generated by  $\ell_i = k_{i+1} \ell_{i+1}$ , so is  $k_{i+1} k_{i+1}$ . Pulling this fact back by  $k_{i+1}$  we have that  $k_{i+1}$  is generated by  $\ell_{i+1}$ . But then  $\ell_i$  is generated by  $\ell_{i+1}$  since

$$\ell_i = k_{i+1} \ell_{i+1}.$$

So  $k_0, \dots, k_i$  are also generated by  $\ell_{i+1}$ . Also, since  $\ell_i$  is an  $i$ th root of  $k_0$ , we have that  $\ell_{i+1} = k_{i+1}^{-1}(\ell_i)$  is an  $i$ th root of  $k_{i+1}^{-1}(k_0)$ . On the other hand,  $k_{i+1}$  is an iterated square root of  $k_0$ , so  $k_{i+1}^{-1}(k_0)^2 = k_0$  by Lemma 15. Thus,

$$\ell_{i+1}^{(i+1)} = k_{i+1}^{-1}(\ell_i^{(i+1)}) = k_{i+1}^{-1}(k_0^{(1)}) = k_0.$$

So  $\ell_{i+1}$  is an  $i+1$ th root of  $k_0$  as desired and we have proved the induction step.  $\square$

We note the following interesting corollary of Lemma 43.

**Corollary 45.** *Suppose that  $S \subseteq \mathcal{E}_\lambda$  is finite, rigid, and weakly square-full. Then  $\langle S \rangle$  embeds into  $\mathcal{A}_1$ .*

**Lemma 46** (The rigidity extension lemma). *If  $S \subseteq \mathcal{E}_\lambda^{2m}$  is a set of elementary embeddings with  $|S| < m$  such that  $S$  is finite, rigid, and weakly square-full, then for any  $k \in S$ , there is a set  $S' \supseteq S$  with the following properties:*

1. *The elements of  $S'$  have a lower bound on their strength (degree of elementarity):  $S' \subseteq \mathcal{E}_\lambda^{2(m-|S|)}$ ;*
2. *The set  $S'$  is finite, rigid, and weakly square-full; and*
3. *The natural pullback by  $S'$  is in  $\mathcal{E}_\lambda^{2(m-|S|)}$  and is an  $n$ th root of  $k$  for some  $n < |S|$ .*

*Proof.* Suppose that  $S = \{k_0, k_1, \dots, k_{|S|-1}\}$  where for all  $i < j$ ,  $k_i \in \text{rng } k_j$ . The natural pullback  $\ell$  given by  $S$  is an  $(|S|-1)$ -th root of  $k_0$ . Let  $k = k_p \in S$ . Then  $k_p$  is an  $m'$ th root of  $k_0$  for some  $m' \leq p$  by Lemma 42. Let  $\ell_{m'-1}, \ell_{m'-2}, \dots, \ell_0$  be given by the proof of Lemma 34 such that:

1. For all  $i < m'$ ,  $\ell_i \in \mathcal{E}_\lambda^{2(m-|S|+i)}$
2.  $\ell_{m'-1}$  is a square root of  $k$
3.  $\ell_i$  is a square root of  $\ell_{i+1}$  for all  $i < m' - 1$

4. For all  $i < m'$ ,  $S \subseteq \text{rng } \ell_i$ .

It is straightforward to check that  $S' = S \cup \{\ell_0, \dots, \ell_{m'-1}\}$  has the desired properties. In particular, we want to show that the natural pullback by  $S'$ , call it  $\ell'$ , is an  $n$ th root of  $k = k_p$  for some  $n < |S|$ . To see this, we have  $\ell$  (the natural pullback given by  $S$ ) is an  $m$ th root of  $k_0$  for  $m < |S|$ . We have that

$$\ell' = (\ell_{m'-1} \circ \dots \circ \ell_0)^{-1}(\ell).$$

Lemma 15 restated in terms of pullbacks implies for  $i < m'$  that

$$\ell_i^{-1}(k^{(i+1)}) = k^{(i)}.$$

So we have that

$$(\ell_{m'-1} \circ \dots \circ \ell_0)^{-1}(k_0) = (\ell_{m'-1} \circ \dots \circ \ell_0)^{-1}(k^{(m')}) = k.$$

So  $\ell'$  is an  $m$ th root of  $k$ . Since  $m < |S|$ , we have what we wanted.  $\square$

The following corollary isolates the property we need below of rigid, weakly square-full sets.

**Corollary 47.** *If  $S \subseteq \mathcal{E}_\lambda^{2m}$  with  $|S| < m$  is a set of elementary embeddings which is finite, rigid, and weakly square-full, then for any  $k \in S$ , there is  $\ell \in \mathcal{E}_\lambda^{2(m-|S|)}$ , a  $(< |S|)$ -iterated root of  $k$  such that  $S \subseteq \mathcal{A}_\ell$ .*

## 5.2 A Canonical Extension of $\mathcal{A}_1$

We showed in the last subsection that  $\mathcal{A}_1$  answers Question 37 in the affirmative for finite, rigid, and weakly square-full sets of embeddings  $E$ . It is natural to ask whether this property can be extended beyond such sets. Countable, rigid, and weakly square-full sets do not (assuming large cardinals), however, in general embed into  $\mathcal{A}_1$ , as a consequence of Laver's theorem on critical points: the order type of  $\{\text{crit } k \mid k \in \mathcal{A}_j\}$  is  $\omega$ . To see this, note that any countable rigid set of square roots of a fixed embedding have distinct critical points which are bounded below  $\lambda$  (see [18] for this argument in the context of inverse limits).

We define a natural extension of  $\mathcal{A}_1$  for which we can embed such sets of embeddings (Theorem 63). This algebra moreover has many interesting and useful properties which help in analyzing  $\mathcal{A}_1$ .

**Definition 48.** Let  $\pi : \mathcal{A}_1 \rightarrow \mathcal{A}_1$  be the map  $a \mapsto xa$ , where  $x$  is the generator of  $\mathcal{A}_1$ . We define  $\mathcal{C}_1$  to be the direct limit of  $\mathcal{A}_1 \rightarrow \mathcal{A}_1 \rightarrow \mathcal{A}_1 \rightarrow \dots$ , where every map is  $\pi$ . We write  $x_n$  to mean the image of the generator of the  $n$ -th copy of  $\mathcal{A}_1$  in the direct limit.

**Remark 49.** *Note that  $\mathcal{C}_1$  has many of the same properties as  $\mathcal{A}_1$ . For instance, the  $<_L$  order lifts to a linear ordering of  $\mathcal{C}_1$ . Similarly, for  $a, b \in \mathcal{C}_1$ , there is  $n, m < \omega$  such that  $a^{(n)} = b^{(m)}$ .*

We will show below that we can answer Question 37 using the algebra  $\mathcal{C}_1$  for a certain class of countable subsets of  $\mathcal{E}_\lambda$  (Theorem 63).

**Theorem 50.** *Assume the large cardinal hypothesis: there exists a nontrivial elementary embedding  $V_{\lambda+1} \rightarrow V_{\lambda+1}$ . Then for any  $z \in \mathcal{C}_1$ , the map  $i_z : \mathcal{C}_1 \rightarrow \mathcal{C}_1$  given by  $i_z(t) = zt$  is elementary.*

**Remark 51.** *Theorem 50 seems to go beyond what is asked in Question 37 in the sense that it is showing that (the simply definable algebra)  $\mathcal{C}_1$  as a structure has properties similar to  $\mathcal{E}_\lambda$  under large cardinal assumptions. Note however, that there are some distinctions between the two situations. For instance, if  $\mathcal{E}_\lambda \neq \emptyset$ , then it is not the case that for all  $j \in \mathcal{E}_\lambda$ ,  $j^+ \upharpoonright \mathcal{E}_\lambda : \mathcal{E}_\lambda \rightarrow \mathcal{E}_\lambda$  is elementary. For instance, if  $j$  is such that  $\text{crit } j$  is least possible, then  $j$  has no square roots. But  $jj$  does have a square root (namely  $j$ ).*

In order to prove the theorem above, we need some preliminary lemmas which are variations of our square root existence lemma above.

**Lemma 52.** *Let  $j \in \mathcal{E}_{\lambda+1}$  and  $k \in \mathcal{A}_j$ . Then there is a  $q \in \mathcal{E}_\lambda$  such that for some  $m < \omega$ ,  $q^{(m)} = j$ , and there is some  $\ell \in \mathcal{A}_q$  such that  $\ell$  is a square root of  $k$ , and  $j \in \text{rng } \ell$ .*

Though we will use the above version of the lemma, we will prove a stronger, more technical version (Lemma 55). To state this technical version we need the following definition.

**Definition 53.** Define the function  $\phi_n$  for  $n < \omega$  on words in  $A_1 = \langle x \rangle$  by induction on word length as follows:  $\phi_n(x) = n + 2$  and  $\phi_n(uv) = \phi_n(u) + \phi_{n+\phi_n(u)}(v)$ .

**Remark 54.** *Note the following clearly hold of  $\phi$ :*

1. *If  $n \leq m$  then  $\phi_n(w) \leq \phi_m(w)$  for any word  $w$ .*
2. *For any  $n < \omega$ , if  $u$  is a literal subterm of  $w$  then  $\phi_n(u) \leq \phi_n(w)$ .*

**Lemma 55.** *Fix a term  $w$  in  $A_1$ . For any  $r < \omega$  and  $j, p \in \mathcal{E}_\lambda^{2^r}$  elementary embeddings and  $m < \omega$  such that  $p^{(m)} = j$  and  $r \geq \phi_m(w)$ , if  $k \in \mathcal{A}_j$  as witnessed by  $w$  then there exists a  $q \in \mathcal{E}_\lambda^{2^{(r-\phi_m(w))}}$  such that for some  $n < \phi_m(w)$ ,  $q^{(n)} = p$  and there exists  $\ell \in \mathcal{A}_q$  such that  $\ell$  is a square root of  $k$  and  $p$  is in the range of  $\ell$ . (See Figure 1 (dotted lines indicate the lower embedding generates the higher embedding).)*

*Proof.* We prove this by induction on the length of  $w$ . In the base case  $w = x$  and  $k = j$ . By Lemma 30, there exists  $\ell \in \mathcal{E}_\lambda^{2^{(r-1)}}$  a square root of  $k = j$  such that  $p \in \text{rng } \ell$ . We need to show that there is  $q$  such that  $q^{(n)} = p$  and  $\ell \in \mathcal{A}_q$ . The set  $S = \{j, p^{(m-1)}, p^{(m-2)}, \dots, p, \ell\}$  is rigid and square-full since  $\ell$  is a square root of  $j$  and  $p \in \text{rng } \ell$ . Applying Corollary 47 to  $S$  and  $p$ , there is  $q \in \mathcal{E}_\lambda^{2^{(r-1-(m+1))}}$ , a  $< |S|$  iterated-root of  $p$  such that  $\ell \in \mathcal{A}_p$ . Note that

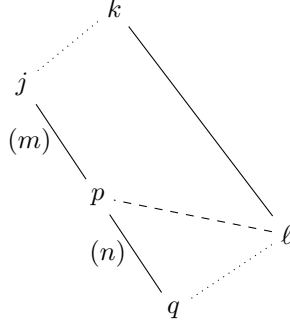


Figure 1: Embedding configuration for Lemma 55. The dotted lines indicate that the embedding higher in the diagram is in the range of the embedding lower in the diagram. The  $(n)$  and  $(m)$  denote an  $n$ - and  $m$ -root, respectively.

$|S| = m + 1$  and  $r - 1 - (m + 1) \geq 0$  since  $r \geq \phi_m(w) = m + 2$ . So the base case follows.

For the general case, we have  $k = uv$  and the induction hypothesis holds for words  $w_u$  and  $w_v$  giving  $u$  and  $v$  (See Figure 2). So  $w = w_u w_v$ . Applying the induction hypothesis on  $j, p$ , and  $u$  all in  $\mathcal{E}_\lambda^{2r}$ , (using that  $\phi_m(w) \geq \phi_m(w_u)$ ), we get  $q_u \in \mathcal{E}_\lambda^{2(r-\phi_m(w_u))}$ ,  $\ell_u$ , and  $n_u < \phi_m(w_u)$  so that  $\ell_u \in A_{q_u}$ ,  $p = q_u^{(n_u)}$ , and  $u = \ell_u^2$ . Noting that  $j = q_u^{(m+n_u)}$ , we again apply the induction hypothesis to  $j, q_u$ , and  $v$  to get  $q_v \in \mathcal{E}_\lambda^{2(r-\phi_m(w_u)-\phi_{m+n_u}(w_v))}$ ,  $\ell_v$ , and  $n_v$  so that  $\ell_v \in A_{q_v}$ ,  $q_u = q_v^{(n_v)}$ , and  $v = \ell_v^2$ . Note that

$$\phi_m(w) = \phi_m(w_u) + \phi_{m+\phi_m(w_u)}(w_v) \geq \phi_m(w_u) + \phi_{m+n_u}(w_v)$$

since  $n_u \leq \phi_m(w_u)$ . So in particular,

$$2(r - \phi_m(w_u) - \phi_{m+n_u}(w_v)) \geq 0$$

and  $q_v \in \mathcal{E}_\lambda^{2(r-\phi_m(w))}$ , as desired.

We claim that  $q = q_v$ ,  $\ell = \ell_u \ell_v$ , and  $n = n_u + n_v$  satisfies the conclusion of the lemma. First, we compute that

$$(\ell_u \ell_v)(\ell_u \ell_v) = \ell_u(\ell_v \ell_v) = \ell_u v = uv = k.$$

The next to last equality follows from the fact that  $v \in \text{rng } \ell_u$ , which in turn follows from  $p \in \text{rng } \ell_u$  and  $v \in A_j = A_{p^{(m)}} \subset A_p$ . Then we show that  $p \in \text{rng } \ell_u \ell_v$ . This follows since  $p, \ell_u \in \text{rng } \ell_v$  implies that  $\ell_u^{-1} p \in \text{rng } \ell_v$ . Applying  $\ell_u$  to both sides we get  $p \in \text{rng } \ell_u \ell_v$ . Lastly, since each of  $\ell_u$  and  $\ell_v$  is in  $A_{q_v}$ ,  $\ell = \ell_u \ell_v$  is also in  $A_q = A_{q_v}$ .  $\square$

**Lemma 56.** *Assume the large cardinal hypothesis: there exists a nontrivial elementary embedding  $V_{\lambda+1} \rightarrow V_{\lambda+1}$ . Then for all  $a, b_0, \dots, b_m \in \mathcal{C}_1$  there exists an  $\bar{a} \in \mathcal{C}_1$  such that  $\bar{a}\bar{a} = a$ ,  $\bar{a}$  left divides  $b_i$  and  $\bar{a}b_i = ab_i$  for all  $i \leq m$ .*

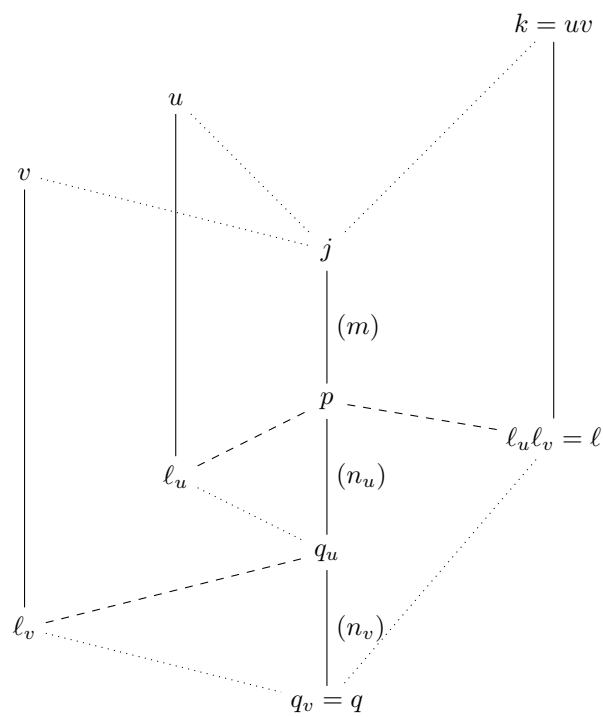


Figure 2: Induction step for Lemma 55.

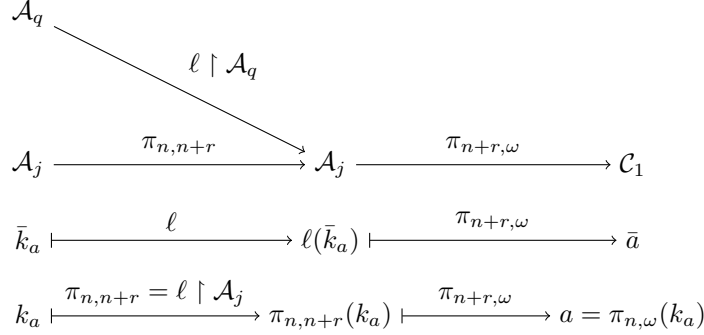


Figure 3: Diagram of the proof of Lemma 56

*Proof.* Recall that  $\mathcal{C}_1$  is the direct limit of the system  $\mathcal{A}_1 \rightarrow \mathcal{A}_1 \rightarrow \dots$  where every map is the embedding  $\pi$  defined by  $x \mapsto xx$ . For any  $j \in \mathcal{E}_\lambda$ , we have  $\mathcal{A}_1 \cong \mathcal{A}_j$ . And hence we can similarly identify  $\mathcal{C}_1$  with the direct limit of  $\mathcal{A}_j \rightarrow \mathcal{A}_j \rightarrow \dots$  where every embedding is defined by  $j \mapsto jj$ .

Fix  $j \in \mathcal{E}_{\lambda+1}$  and let  $\pi_{n,\omega} : \mathcal{A}_j \rightarrow \mathcal{C}_1$  be the natural maps, with  $\pi_{n,m} : \mathcal{A}_j \rightarrow \mathcal{A}_j$  the factor maps for  $n < m$ . We have that  $\pi_{n,m} = j \circ j \circ \dots \circ j$ , with  $(m-n)$ -many compositions. Let  $a, b_0, \dots, b_m \in \mathcal{C}_1$ . Let  $n < \omega$  be such that for some  $k_a$  and  $k_{b_i}$ ,  $\pi_{n,\omega}(k_a) = a$  and  $\pi_{n,\omega}(k_{b_i}) = b_i$  for all  $i \leq m$ .

By Lemma 52, there is a  $q \in \mathcal{E}_\lambda$  such that for some  $r < \omega$ ,  $q^{(r)} = j$  and there is  $\bar{k}_a \in \mathcal{A}_q$  such that  $\bar{k}_a$  is a square root of  $k_a$  and  $j \in \text{rng } \bar{k}_a$  (and hence  $k_{b_0}, \dots, k_{b_m} \in \text{rng } \bar{k}_a$  since these are in  $\mathcal{A}_j$ ).

Let  $\ell = q \circ q \circ \dots \circ q$  where there are  $r$ -many compositions of  $q$ . We have that  $\ell(q) = j$ , and hence  $\ell \upharpoonright \mathcal{A}_q : \mathcal{A}_q \rightarrow \mathcal{A}_j$  is an isomorphism.

We claim that  $\bar{a} = \pi_{n+r,\omega}(\ell(\bar{k}_a))$  satisfies that  $\bar{a}\bar{a} = a$  and  $\bar{a}$  left divides  $b_i$  for all  $i \leq m$ . To see this, note that by Lemma 20 we have  $q \upharpoonright \mathcal{A}_j = j \upharpoonright \mathcal{A}_j$ , and hence

$$\ell \upharpoonright \mathcal{A}_j = \underbrace{q \circ q \circ \dots \circ q}_{r \text{ times}} \upharpoonright \mathcal{A}_j = \underbrace{j \circ j \circ \dots \circ j}_{r \text{ times}} \upharpoonright \mathcal{A}_j = \pi_{n,n+r}.$$

So we have, by elementarity of  $\ell$ , that since  $\bar{k}_a$  is a square root of  $k_a$  that  $\ell(\bar{k}_a)$  is a square root of  $\pi_{n,n+r}(k_a) = \ell(k_a)$ .<sup>9</sup> And hence  $\bar{a} = \pi_{n+r,\omega}(\ell(\bar{k}_a))$  is a square root of

$$\pi_{n+r,\omega}(\pi_{n,n+r}(k_a)) = \pi_{n,\omega}(k_a) = a.$$

A similar computation shows that since  $k_{b_0}, \dots, k_{b_m} \in \text{rng } \bar{k}_a$  that  $\bar{a}$  left divides  $b_0, \dots, b_m$ . This is because for each  $i$ ,  $k_{b_i} \in \text{rng } \bar{k}_a$ , so by elementarity of  $\ell$ ,  $\pi_{n,n+r}(k_{b_i}) = \ell(k_{b_i}) \in \text{rng } \ell(\bar{k}_a)$ . By elementarity of  $\pi_{n+r,\omega}$ ,  $b_i = \pi_{n+r,\omega}(\pi_{n,n+r}(k_{b_i}))$  is in the range of  $\bar{a} = \pi_{n+r,\omega}(\ell(\bar{k}_a))$ . By Lemma 26 the full result follows. See Figure 3.  $\square$

<sup>9</sup>Note here that we cannot apply  $\pi_{n,n+r}$  to  $\bar{k}_a$ .

*Proof of Theorem 50.* By induction on complexity of  $\phi$ , suppose that  $z, c_0, \dots, c_n \in \mathcal{C}_1$  and  $\mathcal{C}_1 \models \exists y \phi[z \cdot c_0, \dots, z \cdot c_n, y]$ . Let  $b \in \mathcal{C}_1$  be a witness to this statement; we want to find a witness in  $z\mathcal{C}_1$ . We have by Lemma 56 that there is  $\bar{z}$  a square root of  $z$  such that  $\bar{z}c_i = zc_i$  for all  $i \leq n$  and  $\bar{z}$  left-divides  $b$ , say  $b = \bar{z}\bar{b}$ . We then have that by our inductive hypothesis,

$$\phi[zc_0, \dots, zc_n, \bar{z}b] \implies \phi[\bar{z}c_0, \dots, \bar{z}c_n, \bar{z}b] \implies \phi[c_0, \dots, c_n, \bar{b}].$$

Pushing forward by  $z$  we have that  $\mathcal{C}_1 \models \phi[zc_0, \dots, zc_n, z\bar{b}]$  as desired.  $\square$

**Corollary 57.** *Assume the large cardinal hypothesis: there exists a nontrivial elementary embedding  $V_{\lambda+1} \rightarrow V_{\lambda+1}$ . Let  $z, a_0, \dots, a_n \in \mathcal{C}_1$ . Assume  $\phi$  is a formula such that  $\exists x \phi[x, a_0, \dots, a_n]$  holds in  $\mathcal{C}_1$ . Also, assume that  $z$  left-divides each  $a_0, \dots, a_n$ . Then there exists some  $x^* \in \mathcal{C}_1$  satisfying  $\phi[x^*, a_0, \dots, a_n]$  such that  $z$  left-divides  $x^*$ .*

*Proof.* This follows by applying the Tarski-Vaught test to the pointwise image of the application embedding given by  $z$ . More precisely, suppose  $a_i = z\bar{a}_i$  for  $i \in \{0, \dots, n\}$ . By Theorem 50,  $\mathcal{C}_1 \models \exists x \phi[x, \bar{a}_0, \dots, \bar{a}_n]$ . Let  $x \in \mathcal{C}_1$  witness this, so  $\mathcal{C}_1 \models \phi[x, \bar{a}_0, \dots, \bar{a}_n]$ . Now apply Theorem 50 to the map  $y \mapsto zy$ , we have  $\mathcal{C}_1 \models \phi[zx, z\bar{a}_0, \dots, z\bar{a}_n]$ . Since  $z\bar{a}_i = a_i$  for  $i \in \{0, \dots, n\}$  and  $z$  left divides  $zx$ , we are done.  $\square$

**Corollary 58.** *Assume the large cardinal hypothesis: there exists a nontrivial elementary embedding  $V_{\lambda+1} \rightarrow V_{\lambda+1}$ . Suppose  $\varphi(x)$  is a first-order formula (with exactly one free variable) and that  $\mathcal{C}_1 \models \exists x \varphi(x)$  then  $\mathcal{C}_1 \models \forall x \varphi(x)$ .*

*Proof.* This follows from the property true of  $\mathcal{A}_1$  (and therefore  $\mathcal{C}_1$ ) that for any  $a$  and  $b$ , there are  $n, m < \omega$  such that  $a^{(n)} = b^{(m)}$  (Proposition 16). To see this, let  $x \in \mathcal{C}_1$  be such that  $\mathcal{C}_1 \models \varphi(x)$  and let  $y$  be any element of  $\mathcal{C}_1$ . Let  $a, b \in \mathcal{A}_1$  be the preimages of  $x, y$  respectively, as usual. Let  $m, n < \omega$  be such that  $a^{(m)} = b^{(n)}$ . Then we have  $x^{(m)} = y^{(n)}$ . By induction, using the elementarity of the maps  $i_z : \mathcal{C}_1 \rightarrow \mathcal{C}_1$  given by  $i_z(t) = zt$  for any  $z \in \mathcal{C}_1$  as given by Theorem 50, we get that  $\mathcal{C}_1 \models \varphi(x^{(m)})$ , so  $\mathcal{C}_1 \models \varphi(y^{(n)})$ . This implies, again by Theorem 50, that  $\mathcal{C}_1 \models \varphi(y)$ .  $\square$

Note that the maps  $i_z : \mathcal{C}_1 \rightarrow \mathcal{C}_1$  for  $z \in \mathcal{C}_1$  given by  $i_z(t) = zt$  are elementary (by Theorem 50) but are never onto. This is because  $\text{rng } i_z \subseteq (z, \infty)$ , where  $(z, \infty) = \{a \in \mathcal{C}_1 \mid z < a\}$ . We can however find automorphisms<sup>10</sup> of  $\mathcal{C}_1$  which map any given element to any other element, which is a stronger version of Corollary 58.

**Theorem 59** (Homogeneity of  $\mathcal{C}_1$ ). *Suppose  $\mathcal{E}_{\lambda+1} \neq \emptyset$ . For any  $a, b \in \mathcal{C}_1$ , there is an automorphism  $\pi : \mathcal{C}_1 \rightarrow \mathcal{C}_1$  such that  $\pi(a) = b$ .*

This theorem follows from the following lemma.

<sup>10</sup>An automorphism of  $\mathcal{C}_1$  is an embedding that is also a bijection.

**Lemma 60.** *Suppose  $\mathcal{E}_{\lambda+1} \neq \emptyset$ . For any  $a \in \mathcal{C}_1$  there is a sequence  $\langle a_n \mid n < \omega \rangle$  of elements of  $\mathcal{C}_1$  such that*

1.  $a_0 = a$ ,
2. for all  $n < \omega$ ,  $a_{n+1}$  is a square root of  $a_n$ ,
3.  $\bigcup_{n < \omega} \mathcal{A}_{a_n} = \mathcal{C}_1$ .

*Proof.* We will prove the lemma with the sequence  $\langle a_n \rangle$  satisfying that  $a_{n+1}$  is an iterated square root of  $a_n$ , from which the original statement follows immediately (by simply including the intervening square roots).

Let  $j : V_{\lambda+1} \rightarrow V_{\lambda+1}$  be an elementary embedding. We realize  $\mathcal{C}_1$  as the direct limit of  $(\pi_n : A^{(n)} \rightarrow A^{(n+1)} : n < \omega)$  where for each  $n$ ,  $A^{(n)} = \langle x_n \rangle$  and  $\pi_n(x_n) = x_{n+1}x_{n+1}$ . Let  $\pi_{n,\omega}$  be the natural direct limit maps.

We have that  $\bigcup_{n < \omega} \mathcal{A}_{\pi_{n,\omega}(x_n)} = \mathcal{C}_1$ , and hence given  $a \in \mathcal{C}_1$ , it is enough to define a sequence  $a_n$  of iterated square roots of  $a$  such that each  $x_n^* = \pi_{n,\omega}(x_n)$  is in  $\mathcal{A}_{a_n}$  for large enough  $n$ . We assume without loss of generality that  $a$  is an iterated root of  $x_0^*$  (using Proposition 16). Let  $t < \omega$  be such that  $a^{(t)} = x_0^*$ .

We define the sequence  $\langle a_n \mid n < \omega \rangle$  by induction such that  $x_n^* \in \mathcal{A}_{a_n}$ . Let  $a_0 = a$ . Suppose  $\langle a_i \mid i \leq n \rangle$  is defined such that  $x_n^* \in \mathcal{A}_{a_n}$ , and there is  $n' < \omega$  such that  $a_n^{(n')} = a_0 = a$ . Define  $a_{n+1}$  as follows. Assume that  $m \geq n+1$  is least such that  $a_n \in \mathcal{A}_{x_m^*}$ . Let  $\sigma : \mathcal{A}_{x_m^*} \rightarrow \mathcal{A}_j$  be the natural isomorphism (see Figure 4). Then  $\sigma(x_m^*) = j$  and we let  $\sigma(a_n) = k$ . Let  $S = \{j^{(m)}, j^{(m-1)}, \dots, j, k^*\}$  where  $k^* \in \mathcal{E}_\lambda^{2(2(m+2)+t+n'+3)}$  is a square root of  $k$  (given by Lemma 33) such that  $j \in \text{rng } k^*$ . Since  $a$  is an iterated root of  $x_0^*$  we have that  $k$  and hence  $k^*$  are iterated roots of  $j^{(m)}$ . So  $S$  is rigid and weakly square-full. By Lemma 46 (since  $|S| = m+2 < m+3$ ) there is an  $\ell \in \mathcal{E}_\lambda^{2(m+2+t+n'+3)}$  a ( $< |S|$ )-iterated root of  $k^*$  such that  $S \subseteq \mathcal{A}_\ell$ . Now let  $j^*$  be a square root of  $j$  such that  $\ell \in \text{rng } j^*$ . We have that for  $s$  such that  $\ell^{(s)} = j^{(m)}$  that  $S' = \{\ell^{(s)}, \ell^{(s-1)}, \dots, \ell, j^*\}$  is a rigid, weakly square-full set. We have

$$|S'| = s+2 < (|S| + 1 + t + n') + 2 = m+3 + t + n' + 2,$$

which is clear by looking at the diagram. And hence again by Lemma 46, there is a  $\bar{j} \in \mathcal{E}_\lambda$  an iterated root of  $j^*$  such that  $S' \subseteq \mathcal{A}_{\bar{j}}$ .

Let  $u < \omega$  be such that  $\bar{j}^{(u)} = j^{(m)}$ , and let  $\bar{a}_{n+1}$  be the image of  $\ell$  under the natural isomorphism  $\sigma^* : \mathcal{A}_{\bar{j}} \cong A^{(u)}$ . Then set  $a_{n+1} = \pi_{u,\omega}(\bar{a}_{n+1})$ .

We claim that  $a_{n+1}$  has the desired property, namely that  $x_{n+1}^* \in \mathcal{A}_{a_{n+1}}$ . To see this, note that  $\pi_{u,\omega}(\sigma^*(\bar{j})) = x_u^*$ . And since  $j \in \mathcal{A}_\ell$ ,  $x_m^* \in \mathcal{A}_{a_{n+1}}$ . So since  $m \geq n+1$ , the desired result follows.  $\square$

*Proof of Theorem 59.* Given  $a, b \in \mathcal{C}_1$ , let  $\langle a_n \mid n < \omega \rangle$  and  $\langle b_n \mid n < \omega \rangle$  be such that:

1.  $a_0 = a$ ,  $b_0 = b$ ,
2. for all  $n < \omega$ ,  $a_{n+1}$  is a square root of  $a_n$  and  $b_{n+1}$  is a square root of  $b_n$ ,

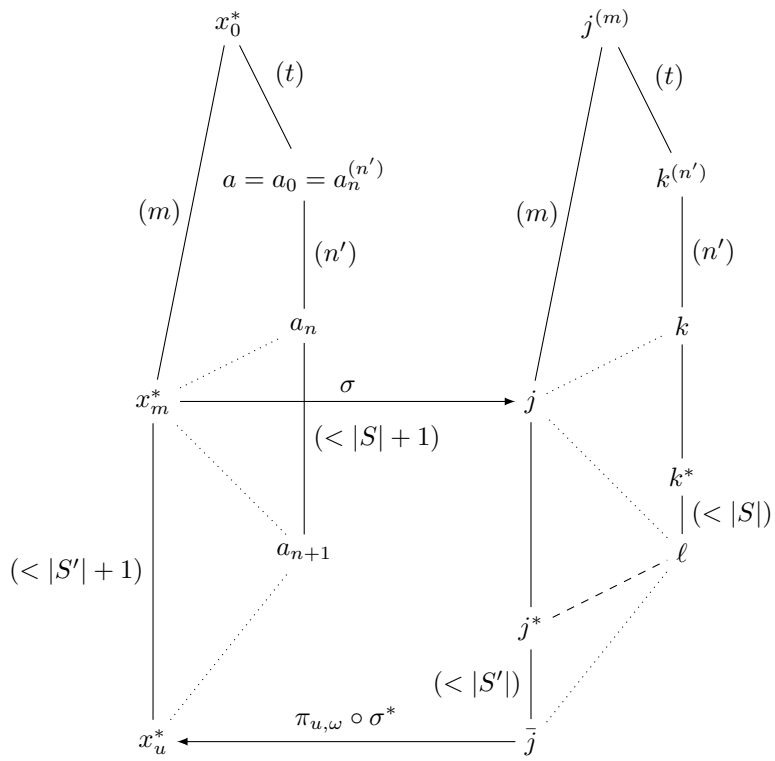


Figure 4: Induction step for Lemma 60.

$$3. \bigcup_{n < \omega} \mathcal{A}_{a_n} = \bigcup_{n < \omega} \mathcal{A}_{b_n} = \mathcal{C}_1.$$

Then the map sending  $a_n \mapsto b_n$  for all  $n < \omega$  clearly induces an automorphism of  $\mathcal{C}_1$  such that  $a \mapsto b$ .  $\square$

Recall that a structure  $A$  is said to be *strongly  $\lambda$ -homogeneous* if for every  $\bar{a}, \bar{b} \in A$  with  $|\bar{a}|, |\bar{b}| < \lambda$ , if  $\bar{a}$  and  $\bar{b}$  have the same type, then there is an automorphism of  $A$  sending  $\bar{a}$  to  $\bar{b}$  [11].

**Corollary 61.** *Suppose  $\mathcal{E}_{\lambda+1} \neq \emptyset$ . Then  $\mathcal{C}_1$  is strongly  $\omega$ -homogeneous.*

*Proof.* Suppose  $\vec{a} = \langle a_0, \dots, a_n \rangle$  and  $\vec{b} = \langle b_0, \dots, b_n \rangle$  are finite tuples from  $\mathcal{C}_1$  which have the same type. Let  $a^* \in \mathcal{C}_1$  be such that  $\vec{a} \subseteq \mathcal{A}_{a^*}$ . Let  $w_i$  for  $i \leq n$  be words such that  $w_i[a^*] = a_i$  for all  $i \leq n$ . Since  $\vec{a}$  and  $\vec{b}$  have the same type, there must be a  $b^* \in \mathcal{C}_1$  such that  $w_i[b^*] = b_i$  for all  $i \leq n$ .

By Theorem 59 there is an automorphism  $\pi : \mathcal{C}_1 \rightarrow \mathcal{C}_1$  such that  $\pi(a^*) = b^*$ . But then  $\pi$  must map  $\vec{a}$  to  $\vec{b}$ , as desired.  $\square$

**Corollary 62** (Universality of  $\mathcal{C}_1$ ). *Let  $\mathcal{C}'_1$  be the direct limit of the system  $(\pi'_n : \mathcal{A}'^{(n)} \rightarrow \mathcal{A}'^{(n+1)} : n < \omega)$  where for each  $n$ ,  $\mathcal{A}'^{(n)} = \langle x'_n \rangle$  is an isomorphic copy of  $\mathcal{A}_1$  and  $\pi'_n(x'_n) = t_n(x'_{n+1})$  for some term  $t_n$ . Then there is an embedding of  $\mathcal{C}'_1$  into  $\mathcal{C}_1$ .*

*Proof.* We will define an embedding  $\sigma : \mathcal{C}'_1 \rightarrow \mathcal{C}_1$ . We define  $\sigma(\pi'_{n,\omega}(x'_n))$  by induction on  $n$ . Set  $\sigma(\pi'_{0,\omega}(x'_0)) = a$  where  $a$  is an arbitrary element of  $\mathcal{C}_1$ . Suppose now that  $\sigma(\pi'_{k,\omega}(x'_k))$  is defined. By Corollary 58, there is some  $y \in \mathcal{C}_1$  such that  $t_k(y) = \sigma(\pi'_{k,\omega}(x'_k))$ . Define  $\sigma(\pi'_{k+1,\omega}(x'_{k+1})) = y$ .

It is easy to see that  $\sigma$  is an embedding.  $\square$

**Theorem 63.** *Assume  $\mathcal{E}_{\lambda+1} \neq \emptyset$ . Suppose that  $S \subseteq \mathcal{E}_\lambda$  is countable, rigid, square-confluent, and square-full. Then  $\langle S \rangle$  embeds into  $\mathcal{C}_1$ .*

Note that, as mentioned at the beginning of Section 5.2, countable rigid sets of square roots of a fixed embedding do not embed into  $\mathcal{A}_1$ , so Theorem 63 does not hold if we replace  $\mathcal{C}_1$  with  $\mathcal{A}_1$ .

We need the following lemma to prove this theorem.

**Lemma 64.** *Suppose that  $S, T \subseteq \mathcal{E}_\lambda$  are finite, rigid and square-full and  $\phi : S \rightarrow T$  is a bijection preserving squares and the range-ordering. Then there is an induced algebra isomorphism  $\phi^* : \langle S \rangle \rightarrow \langle T \rangle$ .*

The proof of Lemma 64 is very similar to the proof of Lemma 43. The isomorphism  $\phi^*$  is generated by identifying the natural pullbacks of  $S$  and  $T$ , and we must check that this isomorphism agrees with  $\phi$ .

*Proof.* Suppose that  $k_0, k_1, \dots, k_n$  is an enumeration of  $S$  such that for all  $s < t \leq n$ ,  $k_s \in \text{rng } k_t$ , and suppose that  $\bar{k}_0, \bar{k}_1, \dots, \bar{k}_n$  is an enumeration of  $T$  such that for all  $s < t \leq n$ ,  $\bar{k}_s \in \text{rng } \bar{k}_t$ . Note that the bijection  $\phi$  must send  $k_i$  to  $\bar{k}_i$  for all  $i \leq n$  and preserve all the square relationships.

We prove by induction that for  $\ell_0 = k_0$ ,  $\ell_i = (k_1 \circ k_2 \circ \dots \circ k_i)^{-1}(k_0)$ ,  $\bar{\ell}_0 = \bar{k}_0$ , and  $\bar{\ell}_i = (\bar{k}_1 \circ \bar{k}_2 \circ \dots \circ \bar{k}_i)^{-1}(\bar{k}_0)$  where  $1 \leq i \leq n$ , that the embedding  $\phi_i^* : \mathcal{A}_{\ell_i} \rightarrow \mathcal{A}_{\bar{\ell}_i}$  induced by  $\ell_i \mapsto \bar{\ell}_i$ , sends  $k_t \mapsto \bar{k}_t$  for  $t \leq i$ .

The base case is obvious. Now suppose it holds for  $i < n$ . We show it is true for  $i + 1$ . Note that  $\ell_{i+1} = k_{i+1}^{-1}\ell_i$  and  $\bar{\ell}_{i+1} = \bar{k}_{i+1}^{-1}\bar{\ell}_i$ . Now,  $k_{i+1}k_{i+1} \in S$ , and hence it is equal to  $k_t$  for some  $t \leq i$ , and so  $\bar{k}_{i+1}\bar{k}_{i+1} = k_t$  as well. Let  $u$  be a word in  $A_1$  such that  $u[\ell_i] = k_t$  (using Lemma 43). By our induction hypothesis, we have that  $u[\ell_i] = \bar{k}_t$ . Pulling back the statement  $u[\ell_i] = k_t$  by  $k_{i+1}$  we have  $u[\ell_{i+1}] = k_{i+1}$ , and pulling back  $u[\ell_i] = \bar{k}_t$  by  $\bar{k}_{i+1}$  we have  $u[\bar{\ell}_{i+1}] = \bar{k}_{i+1}$ .

Now, note that  $\ell_i = k_{i+1}\ell_{i+1} = u[\ell_{i+1}]\ell_{i+1} = w[\ell_{i+1}]$  for a word  $w$ . Similarly  $\bar{\ell}_i = w[\bar{\ell}_{i+1}]$ . So we have  $\phi_{i+1}^* : \ell_i \mapsto \bar{\ell}_i$ . And hence using the induction hypothesis on  $\phi_i^*$ , which agrees with  $\phi_{i+1}^*$  on  $\{k_0, \dots, k_i\}$ , we have that  $\phi_{i+1}^* : k_t \mapsto \bar{k}_t$  for all  $t \leq i$ .

As our induction succeeds, the lemma immediately follows for  $i = n$ .  $\square$

*Proof of Theorem 63.* Let  $S \subseteq \mathcal{E}_\lambda$  be countable, rigid, square-confluent, and square-full. We consider  $S$  as a tree where we say  $k$  is the parent of  $j$  if  $k$  is the square of  $j$ . Since  $S$  is square-confluent, it is connected as a tree. Let  $k_0 \in S$  be an arbitrary element that is fixed from now on. Considering  $S$  as a countable connected tree, we can enumerate the vertices as  $k_0, k_1, k_2, \dots$ , where every  $k_n$  is either the square (parent) or a square root (child) of some  $k_m$  with  $m < n$ . Defining  $S_n = \{k_0, \dots, k_n\}$  for  $n < \omega$ , we have a sequence of non-empty, finite, rigid, square-full sets  $S_n$  such that  $S_0 \subseteq S_1 \subseteq S_2 \subseteq \dots$  and  $\bigcup_{n < \omega} S_n = S$ . In particular, each  $S_n = S_{n-1} \cup \{k_n\}$  where either  $k_n$  is the square of some (actually, the largest) element of  $S_{n-1}$  or  $k_n k_n \in S_{n-1}$ .

We will prove by induction that there are maps  $\sigma_n : \langle S_n \rangle \rightarrow \mathcal{C}_1$  such that for  $n < m$ ,  $\sigma_m \upharpoonright \langle S_n \rangle = \sigma_n$ . Let  $\pi_{n,\omega} : \mathcal{A}_1 \rightarrow \mathcal{C}_1$  be the usual maps into  $\mathcal{C}_1$ . Since  $S_0 = \{k_0\}$ , we can define  $\rho_0 : \mathcal{A}_{k_0} \rightarrow \mathcal{A}_1$  by sending  $k_0$  to the generator of  $\mathcal{A}_1$  and setting  $\sigma_0 = \pi_{0,\omega} \circ \rho_0$ .

We now describe the induction step. If  $k_{m+1}$  is the square of some element of  $S_m$ , then we have  $\langle S_{m+1} \rangle = \langle S_m \rangle$  and we set  $\sigma_{m+1} = \sigma_m$ .

Now suppose  $k_{m+1}$  is the square root of some element of  $S_m$ . For ease of notation, we re-order  $S_m = \{k_0, k_1, \dots, k_m\}$  so that  $k_{n_1} \in \text{rng } k_{n_2}$  for any  $n_1 < n_2$ . We also write  $k = k_{m+1}$ . We have  $S_{m+1} = S_m \cup \{k\}$  and  $kk = k_i$  for some  $i \leq m$ . Let  $r_k \leq m$  be largest such that  $k_0, \dots, k_{r_k} \in \text{rng } k$ . Let  $a_0, \dots, a_m$  be the images of  $k_0, \dots, k_m$  under  $\sigma_m$ . By Lemma 56 there is an  $a \in \mathcal{C}_1$  which is a square root of  $a_i$  such that  $a$  left divides  $a_0, \dots, a_{r_k}$ . Let  $\phi(b, b_0, \dots, b_{r_k})$  be the statement  $b$  is a square root of  $b_i$  such that  $b$  left divides  $b_0, \dots, b_{r_k}$ . We have then that  $\mathcal{C}_1$  satisfies that there exist some  $b$  such that  $\phi[b, a_0, \dots, a_{r_k}]$ . (Note that  $i \leq r_k$ ).

Suppose first  $r_k < m$ . We have that  $a_{r_k+1}$  left-divides  $a_0, \dots, a_{r_k}$ . By Corollary 57, there is some  $b \in \mathcal{C}_1$ , such that  $\phi[b, a_0, \dots, a_{r_k}]$  holds and  $a_{r_k+1}$  left-divides  $b$ . Since  $\{a_0, \dots, a_m\}$  is rigid, iterated applications of Corollary 57 show that there is a  $b$  such that  $\phi[b, a_0, \dots, a_{r_k}]$  holds and  $b$  is left-divided by  $a_{r_k+1}, a_{r_k+2}, \dots, a_m$ . Fix such a witness  $a^*$ , and let  $T^* = \{a_0, \dots, a_m, a^*\}$ .

For the case that  $r_k = m$ , we let  $a^*$  be any  $b$  such that  $\phi[b, a_0, \dots, a_{r_k}]$ . We then define  $T^*$  in the same way.

Let  $q < \omega$  be least such that  $T^* \subseteq \text{rng } \pi_{q,\omega}$ . Fix  $j \in \mathcal{E}_{\lambda+1}$ . Let  $S^*$  be the set of embeddings in  $\mathcal{A}_j$  corresponding to  $\pi_{q,\omega}^{-1}[T^*]$  under the isomorphism  $\mathcal{A}_j \cong \mathcal{A}_1$ . We have then that  $S^*$  is a finite, rigid, square-full set. Furthermore, there is a natural bijection  $S_{m+1} \rightarrow S^*$  which preserves squares and the range-ordering. So by Lemma 64 there is an induced algebra isomorphism  $\tau : \langle S_{m+1} \rangle \rightarrow \langle S^* \rangle$ . We define  $\sigma_{m+1}$  to be the composition of  $\tau$ , the isomorphism  $\mathcal{A}_j \cong \mathcal{A}_1$ , and  $\pi_{q,\omega}$ . It is easy to check that  $\sigma_{m+1}$  is as desired and agrees with  $\sigma_m$ . So the theorem follows by induction.  $\square$

We mention one more consequence of Lemma 64. In this statement we refer to *rigid* subsets of  $\mathcal{C}_1$  by which we mean the same definition as in the case of elementary embeddings, but with  $j \in \text{rng } k$  replaced by  $a$  left-divides  $b$ . See Section 3.

**Theorem 65.** *Assume the large cardinal hypothesis: there exists a nontrivial elementary embedding  $V_{\lambda+1} \rightarrow V_{\lambda+1}$ . Suppose that  $S, T \subseteq \mathcal{C}_1$  are finite, rigid, and square-full and  $\phi : S \rightarrow T$  is a bijection which preserves squares and the left-divisor ordering. Then  $\phi$  extends to an automorphism of  $\mathcal{C}_1$ .*

*Proof sketch.* Let  $S', T' \subseteq \mathcal{E}_\lambda$  be corresponding sets of embeddings such that there are bijections  $S \rightarrow S'$  and  $T \rightarrow T'$  preserving squares and the left-divisor ordering. The proof of Lemma 64 shows that the natural isomorphism which sends the natural pullback of  $S'$  to the natural pullback of  $T'$  also sends  $S'$  to  $T'$  pointwise (when ordered according to the range relation). Translating this fact back (as in the proof of Theorem 63) into  $\mathcal{C}_1$  and using Theorem 59, there is an automorphism sending the natural pullback of  $S$  to the natural pullback of  $T$ . And hence this automorphism is as desired.  $\square$

## 6 Open Questions and Possible Extensions

Whether or not the large cardinal hypotheses in the above theorems are necessary remains open.

**Question 66.** *Can the conclusions of Theorems 36 (1), 50, and 59 be proven in ZFC? Or do the conclusions of Theorems 36 (1), 50, and 59 imply  $\text{Con}(ZFC)$ ?*

Whether our results on  $\mathcal{C}_1$  can be extended to several generators is also unclear.

**Question 67.** *Is there an analogue of  $\mathcal{C}_1$  for two (or more) generators? In particular, is there a (simply definable) algebra which embeds  $\mathcal{A}_2$  and where application is elementary?*

## References

- [1] Andrew Brooke-Taylor, Scott Cramer, and Sheila K. Miller Edwards. A free two-generated left distributive algebra of embeddings. *arXiv preprint arXiv:2508.02244*, 2024.
- [2] Andrew Brooke-Taylor and Sheila K. Miller Edwards. A free left distributive algebra of elementary embeddings with uncountably many generators. In Preparation, 2026.
- [3] Stanley Burris and H. P. Sankappanavar. *A course in universal algebra*, volume 78 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1981.
- [4] David de la Torre. *On the Finiteness of Certain Left-Distributive Algebras*. 2024. Thesis (M.Sc.)—California State University, Northridge.
- [5] Patrick Dehornoy. Free distributive groupoids. *J. Pure Appl. Algebra*, 61(2):123–146, 1989.
- [6] Patrick Dehornoy. Braid groups and left distributive operations. *Transactions of the American Mathematical Society*, 345(1):115–150, 1994.
- [7] Patrick Dehornoy. *Braids and self-distributivity*, volume 192 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, 2000.
- [8] Randall Dougherty and Thomas Jech. Finite left-distributive algebras and embedding algebras. *Advances in Math*, 130:201–241, 1997.
- [9] Gabriel Goldberg. Choiceless cardinals and the continuum problem. *arXiv preprint arXiv:2201.11557*, 2022.
- [10] Gabriel Goldberg. Measurable cardinals and choiceless axioms. *Annals of Pure and Applied Logic*, 175(1, Part B):103323, 2024. Kenneth Kunen (1943-2020).
- [11] Wilfrid Hodges. *Model theory*, volume 42 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1993.
- [12] Akihiro Kanamori. *The higher infinite*. Perspectives in Mathematical Logic. Springer-Verlag, Berlin, 1994. Large cardinals in set theory from their beginnings.
- [13] David Larue. Braid words and irreflexivity. *Algebra Universalis*, 31:104–112, 1994.
- [14] David Larue. *Left Distributive and Left-Distributive Idempotent Algebras*. PhD thesis, University of Colorado, Boulder, 1994.
- [15] Richard Laver. The left distributive law and the freeness of an algebra of elementary embeddings. *Advances in Mathematics*, 91:209–231, 1992.

- [16] Richard Laver. A division algorithm for the free left distributive algebra. In *Logic Colloquium '90 (Helsinki, 1990)*, volume 2 of *Lecture Notes Logic*, pages 155–162. Springer, Berlin, 1993.
- [17] Richard Laver. On the algebra of elementary embeddings of a rank into itself. *Advances in Math*, 110:334–346, 1995.
- [18] Richard Laver. Implications between strong large cardinal axioms. *Ann. Pure Appl. Logic*, 90(1-3):79–90, 1997.
- [19] Richard Laver and Sheila K. Miller. The free one-generated left distributive algebra: basics and a simplified proof of the division algorithm. *Open Mathematics (formerly the Central European Journal of Mathematics)*, 11(12):2150–2175, 2013.
- [20] Sheila K. Miller. *Free Left Distributive Algebras*. PhD thesis, University of Colorado, Boulder, 2007.
- [21] Sheila K. Miller. Left division in the free left distributive algebra on many generators. *Archive for Mathematical Logic*, 55(1-2):177–205, 2016.
- [22] Farmer Schlutzenberg. On the consistency of ZF with an elementary embedding from  $V_{\lambda+2}$  into  $V_{\lambda+2}$ . *J. Math. Log.*, 25(2):Paper No. 2450013, 43, 2025.
- [23] Alfred Tarski and Hourya Sinaceur. Address at the Princeton University Bicentennial Conference on Problems of Mathematics (December 17-19, 1946). *The Bulletin of Symbolic Logic*, 6(1):1–44, 2000.